

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年7月26日 (26.07.2001)

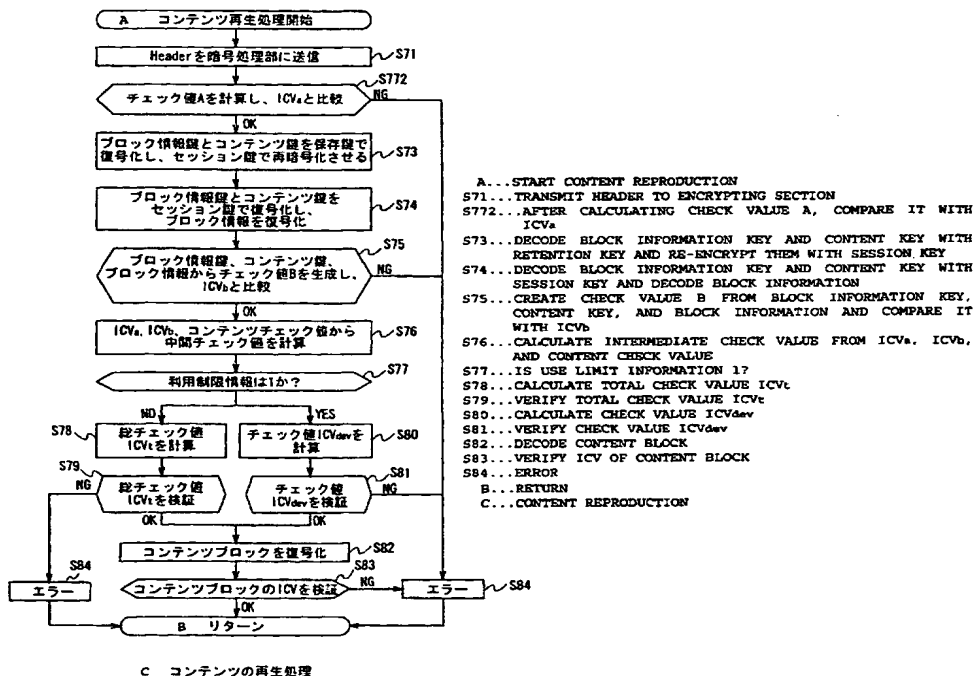
PCT

(10) 国際公開番号
WO 01/54099 A1

- (51) 国際特許分類⁷: G09C 1/00, H04L 9/32 (72) 発明者; および
(75) 発明者/出願人 (米国についてののみ): 浅野智之 (ASANO, Tomoyuki) [JP/JP], 石橋義人 (ISHIBASHI, Yoshihito) [JP/JP], 白井太三 (SHIRAI, Taizo) [JP/JP], 秋下 徹 (AKISHITA, Toru) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/00346
- (22) 国際出願日: 2001年1月19日 (19.01.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2000-013322 2000年1月21日 (21.01.2000) JP
特願2000-015551 2000年1月25日 (25.01.2000) JP
特願2000-015858 2000年1月25日 (25.01.2000) JP
特願2000-016029 2000年1月25日 (25.01.2000) JP
特願2000-016213 2000年1月25日 (25.01.2000) JP
特願2000-016251 2000年1月25日 (25.01.2000) JP
特願2000-016292 2000年1月25日 (25.01.2000) JP
- (74) 代理人: 弁理士 田辺恵基 (TANABE, Shigemoto); 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンファンタジアビル5階 Tokyo (JP).
- (81) 指定国 (国内): AU, BR, CA, CN, KR, MX, NZ, RU, SG, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 添付公開書類:
— 国際調査報告書
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- 2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: DATA AUTHENTICATION SYSTEM

(54) 発明の名称: データ認証処理システム



(57) Abstract: Partial data is verified by checking a partial check value used as a check value for a partial data set of a content, and thereby the whole data set is verified by checking a partial check values used for verifying the partial check value set where partial check values are combined.



(57) 要約:

コンテンツの部分データ集合に対するチェック値としての部分チェック値の照合により部分データの検証処理を実行し、部分チェック値を組み合わせた部分チェック値集合に対する検証を行う部分チェック値検証用チェック値の照合によりデータ集合全体に対する検証処理を実行する。

明 細 書

データ認証処理システム

技術分野

本発明は、データ処理装置およびデータ処理方法に関し、さらに詳細には、データコンテンツを構成するデータの正当性、すなわち改竄の有無を検証する方法、装置、検証値の付与方法に関する。また、暗号処理に必要な個別鍵を、各個別鍵に対応したマスター鍵によって生成することにより、セキュリティを高めることを可能とした装置および方法に関する。また、本発明は、データコンテンツの不正利用を排除する構成を提供するものであり、具体的には、不正再生機器を識別してコンテンツの不正利用を排除することを可能とした装置および方法に関する。さらに本発明は、データ処理装置のみに利用可能なコンテンツと、他のデータ処理装置においても利用可能なコンテンツとをデータ処理装置固有の情報等に基づいて容易に設定することを可能とした装置および方法に関する。さらに、データコンテンツを構成するデータの正当性、すなわち改竄の有無を検証する方法、装置、検証値の付与方法に関する。

さらに、本発明は、音声情報、画像情報、プログラムデータの少なくともいずれかを含むデータを暗号化処理して、各種のヘッダ情報と共にコンテンツ利用者に提供し、コンテンツ利用者が再生、実行、あるいは記録デバイスに対する格納処理等を行なう構成において、コンテンツデータを高いセキュリティ管理のもとに提供および利用することを可能としたコンテンツデータ構成を実現するデータ処理装置、コンテンツデータ生成方法、およびデータ処理方法に関する。

さらに、データコンテンツが圧縮された音声データ、あるいは画像データ等である場合の再生処理を効率的に実行する構成を提供するものであり、具体的には、コンテンツデータの構成を圧縮データと伸長処理プログラムとを組み合わせた構成としたり、適用伸長処理プログラムをヘッダ情報として格納した圧縮データ

コンテンツのヘッダ情報に基づいて適用可能な伸長処理プログラムを検索抽出して再生処理を実行することを可能としたデータ処理装置、データ処理方法およびコンテンツデータ生成方法に関する。

本発明は、DVD、CD等の記憶媒体、あるいはCATV、インターネット、衛星通信等の有線、無線各通信手段等の経路で入手可能な音声、画像、ゲーム、プログラム等の各種コンテンツを、ユーザの所有する記録再生器において再生し、専用の記録デバイス、例えばメモ리카ード、ハードディスク、CD-R等に格納するとともに、記録デバイスに格納されたコンテンツを利用する際、コンテンツ配信側の希望する利用制限を付す構成を実現するとともに、この配布されたコンテンツを、正規ユーザ以外の第三者に不正利用されないようにセキュリティを確保する構成および方法に関する。

背景技術

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体を介して流通している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、ゲーム機器等の記録再生機器に付属する記録デバイス、例えばメモ리카ード、ハードディスク等に格納することが可能であり、一旦格納された後は、格納媒体からの再生により利用可能となる。

従来のビデオゲーム機器、PC等の情報機器において使用されるメモ리카ード装置の主な構成要素は、動作制御のための制御手段と、制御手段に接続され情報機器本体に設けられたスロットに接続するためのコネクタと、制御手段に接続されデータを記憶するための不揮発性メモリ等である。メモ리카ードに備えられた不揮発性メモリはEEPROM、フラッシュメモリ等によって構成される。

このようなメモ리카ードに記憶されたデータ、あるいはプログラム等の様々な

コンテンツは、再生機器として利用されるゲーム機器、P.C等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により不揮発性メモリから呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないうにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化处理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

暗号化データは、所定の手続きによる復号化处理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化处理に暗号化鍵を用い、復号化处理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化处理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化处理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

上述の暗号化处理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパ

スワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはRSA (R i v e s t - S h a m i r - A d l e m a n) 暗号がある。

このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。これらの暗号方式を採用した従来のコンテンツ配布構成について図1を用いて簡単に説明する。

図1は、PC (パーソナルコンピュータ)、ゲーム機器等の再生手段10において、DVD、CD30、インターネット40等のデータ提供手段から取得したプログラム、音声データ、映像データ等 (コンテンツ (C o n t e n t)) を再生するとともに、DVD、CD30、インターネット40等から取得したデータをフロッピーディスク、メモリカード、ハードディスク等の記憶手段20に記憶可能とした構成例を示すものである。

プログラム、音声データ、映像データ等のコンテンツは、暗号化処理がなされ、再生手段10を有するユーザに提供される。正規ユーザは、暗号化データとと

もに、その暗号化、復号化鍵である鍵データを取得する。

再生手段10はCPU12を有し、入力データの再生処理を再生処理部14で実行する。再生処理部14は、暗号化データの復号処理を実行して、提供されたプログラムの再生、音声データ、画像データ等コンテンツ再生を行なう。

正規ユーザは、提供されたプログラムを、再度使用するために記憶手段20にプログラム／データ等、コンテンツの保存処理を行なう。再生手段10には、このコンテンツ保存処理を実行するための保存処理部13を有する。保存処理部13は、記憶手段20に記憶されたデータの不正使用を防止するため、データに暗号化処理を施して保存処理を実行する。

コンテンツを暗号化する際には、コンテンツ暗号用鍵を用いる。保存処理部13は、コンテンツ暗号用鍵を用いて、コンテンツを暗号化し、それをFD（フロッピーディスク）、メモ리카ード、ハードディスク等の記憶手段20の記憶部21に記憶する。

ユーザは、記憶手段20から格納コンテンツを取り出して再生する場合には、記憶手段20から、暗号化データを取り出して、再生手段10の再生処理部14において、コンテンツ復号用の鍵、すなわち復号化鍵を用いて復号処理を実行して暗号化データから復号データを取得して再生する。

図1に示す従来の構成例に従えば、フロッピーディスク、メモ리카ード等の記憶手段20では格納コンテンツが暗号化されているため、外部からの不正読み出しは防止可能となる。しかしながら、このフロッピーディスクを他のPC、ゲーム機器等の情報機器の再生手段で再生して利用しようとする、同じコンテンツ鍵、すなわち暗号化されたコンテンツを復号するための同じ復号化鍵を有する再生手段でなければ再生不可能となる。従って、複数の情報機器において利用可能な形態を実現するためには、ユーザに提供する暗号鍵を共通化しておくことが必要となる。

しかしながら、コンテンツの暗号鍵を共通化することは、正規ライセンスを持たないユーザに暗号処理用の鍵を無秩序に流通させる可能性を高めること

になり、正規のライセンスを持たないユーザによるコンテンツの不正利用を防止できなくなるという欠点があり、正規ライセンスを持たないP C、ゲーム機器等での不正利用の排除が困難になる。

また、コンテンツの暗号鍵、復号鍵を共通化するということは、一つの機器から万一その鍵情報が漏洩した場合に、被害の及ぶ範囲がその鍵を用いているシステム全体となってしまう。

さらに、上述のように鍵を共通化した環境においては、例えばあるP C上で作成され、メモリカード、フロッピーディスク等の記憶手段に保存された暗号化されたコンテンツは、別のフロッピーディスクに容易に複製することが可能であり、オリジナルのコンテンツデータではなく複製フロッピーディスクを用いた利用形態が可能となり、ゲーム機器、P C等の情報機器において利用可能なコンテンツデータが多数複製されたり、または改竄されてしまう可能性があった。

コンテンツデータの正当性、すなわちデータが改竄されていないことをチェックするために検証用のチェック値をコンテンツデータに含ませ、記録再生器において、検証対象のデータに基づいて生成したチェック値とコンテンツデータに含まれるチェック値とを照合処理することによって、データ検証を行なう方法が従来から行なわれている。

しかしながら、データコンテンツに対するチェック値は、データ全体に対して生成されるのが一般的であり、データ全体に対して生成されたチェック値の照合処理を実行するためには、チェック対象となったデータ全体に対するチェック値生成処理を実行することが必要となる。例えばDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)により、チェック値ICVを求める手法を行なう場合、データ全体に対するDES-CBCの処理を実行することが必要となる。この計算量は、データ長が長くなるにつれ増大することとなり、処理効率の点で問題がある。

発明の開示

本発明は、このような従来技術の問題点を解決するものであり、データ正当性の確認処理を効率的に実行し、コンテンツデータの検証処理の効率化、さらに検証後の記録デバイスに対するダウンロード処理、あるいは検証後の再生処理等を効率的に実行することを可能とするデータ処理装置、データ処理方法およびデータ検証値付与方法、並びにプログラム提供媒体を提供することを第1の目的とする。

また、コンテンツデータの利用を正当な利用者に限定する手法としてデータ暗号化、データ復号化、データ検証、認証処理、署名処理等、各種の暗号処理があるが、これら各種の暗号処理を実行するためには、2つの装置間、すなわち、コンテンツデータを転送する装置間、あるいは認証処理を実行する装置間において、共有する秘密情報、例えばコンテンツデータの暗号化、復号化に適用する鍵情報を共有したり、認証する装置間で認証に使用する認証鍵を共有することが必要となる。

従って例えば、2つの装置のいずれかから、その共有秘密情報である鍵データが漏洩した場合には、その共有鍵情報を用いたコンテンツの暗号化データは、ライセンスを持たない第三者によっても復号可能となり、不正なコンテンツの利用が可能となってしまう。また認証鍵が漏洩した場合にも同様であり、全くライセンスを持たない装置に対する認証が成立してしまい、鍵の漏洩は、システム全体を脅かす結果をもたらす。

本発明は、このような問題点を解決するものである。本発明のデータ処理装置、データ処理システム、およびデータ処理方法は、データ暗号化、データ復号化、データ検証、認証処理、署名処理等の暗号処理を実行するために必要となる個別鍵を記憶部に記憶格納せず、これらの個別鍵を生成するためのマスター鍵を記憶部に格納し、暗号処理部がマスター鍵と、装置またはデータの識別データに基づいて必要な個別鍵を生成することにより、暗号処理におけるセキュリティを高めたデータ処理装置、データ処理システム、およびデータ処理方法を提供することを第2の目的とする。

また、コンテンツデータは、暗号化されて提供することにより、ある程度のセキュリティを保持することが可能であるが、メモリに格納された様々な暗号鍵がメモリの不正な読み取りにより予も取られ、鍵データ等が流出し、正規なライセンスのされていない記録再生器にコピーされた場合、コピーされた鍵情報によって不正なコンテンツ利用がなされる可能性がある。

本発明は、このような不正な再生機器の排除を可能とした構成、すなわち不正な再生機器を識別し、識別された不正機器においては、コンテンツデータの再生、ダウンロード等の処理を実行させない構成としたデータ処理装置、データ処理方法およびコンテンツデータ生成方法を提供することを第3の目的とする。

また、コンテンツデータの利用を正当な利用者に限定する手法として所定の暗号化鍵を用いた暗号処理、例えば署名処理があるが、従来の署名による暗号処理は、署名鍵がコンテンツを利用するシステムのエンティティのすべてにおいて共通化されているものが一般的であり、このような署名鍵では、異なる装置で共通のコンテンツを利用することが可能となり、コンテンツの不正コピーが発生する等の問題がある。

独自のパスワード等を用いてコンテンツを暗号化して格納することも可能であるが、パスワードは盗まれる可能性もあり、また、異なる再生器を介して同一のパスワードを入力することによって、同じ暗号化コンテンツデータを復号することが可能であり、従来のセキュリティ構成においては、再生器を識別して、その再生器にのみ利用可能なシステムを実現することが困難だった。

本発明は、このような従来技術の問題点を解決するものであり、本発明の構成においては、データ処理装置固有の装置固有鍵と、コンテンツデータを利用する他のデータ処理装置に共通のシステム共通鍵とを選択的に利用可能とすることにより、コンテンツの利用制限に応じて、特定のデータ処理装置においてのみコンテンツを再生することを可能としたデータ処理装置およびデータ処理方法を提供することを第4の目的とする。

また、コンテンツデータは、音声情報、画像情報、プログラムデータ等様々な

種類があり、また、コンテンツデータのすべてを暗号化する場合や、暗号化処理の必要な部分と暗号化処理の不要な部分とが混在する場合等、様々なコンテンツが存在する。

このような、様々なコンテンツに対して、一律に暗号化処理を適用することは、その再生処理において不要な復号処理を発生させたり、処理効率、処理速度の点で好ましくない事態が発生する場合がある。例えば音楽データのようなリアルタイム再生が必須となるデータ等には処理速度の速い復号処理可能なコンテンツデータ構成とすることが望まれる。

本発明は、このような問題点を解決するものである。本発明のデータ処理装置、コンテンツデータ生成方法、およびデータ処理方法は、コンテンツデータの種別に応じた様々なコンテンツデータ構成、すなわちコンテンツに応じた異なる複数のデータフォーマットをコンテンツに適用することを可能とし、セキュリティが高くかつ再生、実行等において利用しやすいコンテンツデータの生成および処理を可能としたデータ処理装置、コンテンツデータ生成方法、およびデータ処理方法を提供することを第5の目的とする。

また、復号された音声データ、画像データ等は、AV出力部に出力されて再生される。しかし、昨今多くのコンテンツは圧縮処理がなされて記憶媒体に格納、あるいは配信されることが多い。従って再生処理の前に、これらの圧縮データを伸長処理することが必要となる。例えば音声データであってMP3圧縮がなされていれば、MP3デコーダによって音声データの復号処理がなされて出力される。また、コンテンツデータが画像データであり、MPEG2圧縮画像であれば、MPEG2デコーダによって伸長処理が実行された後、出力されることになる。

しかしながら、圧縮処理、伸長処理プログラムには、様々な種類があり、コンテンツプロバイダから媒体、ネットワーク等を介して圧縮データを提供されても、再生装置内に対応する伸長処理実行プログラムが無い場合は、これを再生することができないという事態が発生する。

本発明は、圧縮データの再生処理を効率的に実行する構成、すなわち、コンテ

ンツが圧縮された音声データ、あるいは画像データ等である場合の再生処理を効率的に実行するデータ処理装置、データ処理方法およびコンテンツデータ生成方法を提供することを第6の目的とする。

本発明の第1の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、上記コンテンツデータに対する暗号処理を実行する暗号処理部と、上記暗号処理部に対する制御を実行する制御部とを有し、上記暗号処理部は、コンテンツデータ構成部を複数部分に分割した部分データを1以上含む部分データ集合に対するチェック値として部分チェック値を生成し、該生成した部分チェック値の照合処理により上記部分データの検証処理を実行するとともに、少なくとも上記部分チェック値を1以上含む部分チェック値集合データ列に基づいて中間チェック値を生成し、該生成した中間チェック値を用いて、上記部分チェック値集合を構成する複数の部分チェック値に対応する複数の部分データ集合全体に対する検証処理を実行する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記部分チェック値は、チェック対象となる部分データをメッセージとし、部分チェック値生成鍵を適用した暗号処理によって生成される値であり、上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとし、総チェック値生成鍵を適用した暗号処理によって生成される値であり、上記暗号処理部は、上記部分チェック値生成鍵および上記総チェック値生成鍵を格納した構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、生成する部分チェック値に対応する複数種類の部分チェック値生成鍵を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理はDES暗号処理であり、上記暗号処理部は、DES暗号処理を実行可能な構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記部分チェック値は、チェック対象となる部分データをメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、上記暗号処理部は、DES-CBCモードによる暗号処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部の有するDES-CBCモードによる暗号処理構成は、処理対象となるメッセージ列の一部においてのみトリプルDESが適用される構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、署名鍵を有し、上記暗号処理部は、上記中間チェック値に対して上記署名鍵を適用した暗号処理により生成される値をデータ検証のための照合値として適用する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、署名鍵として異なる複数の署名鍵を有し、上記暗号処理部は、上記コンテンツデータの利用制限態様に応じて上記異なる複数の署名鍵から選択された署名鍵を上記中間チェック値に対する暗号処理に適用してデータ検証のための照合値とする構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、上記複数の署名鍵として、データ検証処理を実行するシステムの全エンティティに共通の共通署名鍵と、データ検証処理を実行する各々の装置固有の装置固有署名鍵とを有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッダ部分チェック値と、データの一部を構成するコンテンツブロックデータについて生成される1以上のコンテンツチェック値とを含み、上記暗号処理部は、上記

ヘッダ部内データの部分データ集合について1以上のヘッダ部分チェック値を生成して照合処理を実行し、上記コンテンツ部内データの部分データ集合について1以上のコンテンツチェック値を生成して照合処理を実行し、さらに、生成された上記ヘッダ部分チェック値および上記コンテンツチェック値全てに基づいて総チェック値を生成して照合処理を実行することによりデータ検証を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッダ部分チェック値を含み、上記暗号処理部は、上記ヘッダ部内データの部分データ集合について1以上のヘッダ部分チェック値を生成して照合処理を実行し、さらに、生成された上記1以上のヘッダ部分チェック値および上記データの一部を構成するコンテンツブロックデータからなるデータ列に基づいて総チェック値を生成して照合処理を実行することによりデータ検証を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、上記暗号処理部において正当性検証の実行されたデータを格納する記録デバイスを有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部における部分チェック値の照合処理において、照合が成立しなかった場合において、上記制御部は、上記記録デバイスへの格納処理を中止する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、上記暗号処理部において正当性検証の実行されたデータを再生する再生処理部を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、上記暗号処理部における部分チェック値の照合処理において、照合が成立しなかった場合において、上記制御部は、上記再生処理部での再生処理を中止する

構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、上記暗号処理部における部分チェック値の照合処理において、データのヘッダ部分チェック値の照合処理のみを実行し、ヘッダ部分チェック値の照合が成立したデータを上記再生処理部に転送して再生可能とする制御手段を有することを特徴とする。

さらに、本発明の第2の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、上記コンテンツデータに対する暗号処理を実行する暗号処理部と、上記暗号処理部に対する制御を実行する制御部とを有し、上記暗号処理部は、検証対象データが暗号化データである場合、該暗号化データの復号処理によって得られる復号データに対して演算処理を実行して得られる演算処理結果データに対して署名鍵を適用した暗号処理を施すことにより、該検証対象データのチェック値を生成する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記演算処理は、上記暗号化データの復号処理によって得られる復号データを所定バイト単位で排他的論理和演算する処理であることを特徴とする。

さらに、本発明の第3の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法において、コンテンツデータ構成部を複数部分に分割した部分データを1以上含む部分データ集合に対するチェック値として部分チェック値を生成し、該生成部分チェック値を照合する処理により上記部分データの検証処理を実行し、少なくとも上記部分チェック値を1以上含む部分チェック値集合データ列に基づいて中間チェック値を生成し、該生成中間チェック値を用いて上記部分チェック値集合を構成する複数の部分チェック値に対応する複数の部分データ集合全体に対する検証処理を実行することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値

は、チェック対象となる部分データをメッセージとし、部分チェック値生成鍵を適用した暗号処理によって生成される値であり、上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとし、総チェック値生成鍵を適用した暗号処理によって生成される値であることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値は、生成する部分チェック値に対応する異なる種類の部分チェック値生成鍵を適用して生成することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記暗号処理はDES暗号処理であることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値は、チェック対象となる部分データをメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、さらに、上記中間チェック値に対して署名鍵を適用した暗号処理により生成される値をデータ検証のための照合値として適用することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、データの利用制限態様に応じて異なる署名鍵を上記中間チェック値に対する暗号処理に適用してデータ検証のための照合値とすることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記署名鍵として、データ検証処理を実行するシステムの全エンティティに共通の共通署名鍵と、データ検証処理を実行する各々の装置固有の装置固有署名鍵とをデータの利用制限態様に応じて選択して使用することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッ

ダ部分チェック値と、データの一部を構成するコンテンツ部内データについて生成される1以上のコンテンツチェック値とを含み、データ検証処理は、上記ヘッダ部内データの部分データ集合について1以上のヘッダ部分チェック値を生成して照合処理を実行し、上記コンテンツ部内データの部分データ集合について1以上のコンテンツチェック値を生成して照合処理を実行し、さらに、生成された上記ヘッダ部分チェック値および上記コンテンツチェック値全てに基づいて総チェック値を生成してデータ検証を実行するものであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッダ部分チェック値を含み、データ検証処理は、上記ヘッダ部内データの部分データ集合について1以上のヘッダ部分チェック値を生成して照合処理を実行し、さらに、生成された上記1以上のヘッダ部分チェック値および上記データの一部を構成するコンテンツブロックデータからなるデータ列に基づいて総チェック値を生成して照合処理を実行することによりデータ検証を実行するものであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、データの検証後、さらに、検証済みデータを記録デバイスに格納する処理を含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値の照合処理において、照合が成立しなかった場合において、上記記録デバイスへの格納処理を中止する制御を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、データの検証後、データを再生するデータ再生処理を含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値の照合処理において、照合が成立しなかった場合において、上記再生処理部での再生処理を中止する制御を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記部分チェック値の照合処理において、データのヘッダ部分チェック値の照合処理のみを実行し、

ヘッダ部分チェック値の照合が成立したデータを上記再生処理部に転送して再生可能とする制御を実行することを特徴とする。

さらに、本発明の第4の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法であり、検証対象データが暗号化データである場合、該暗号化データの復号処理によって得られる復号データに対して演算処理を実行し、上記演算処理によって得られる演算処理結果データに対して署名鍵を適用した暗号処理を実行することにより上記検証対象データのチェック値を生成することを徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記演算処理は、上記暗号化データの復号処理によって得られる復号データを所定バイト単位で排他的論理和演算する処理であることを特徴とする。

さらに、本発明の第5の側面は、データ検証処理のためのデータ検証値付与方法であり、データを複数部分に分割した部分データを1以上含む部分データ集合に対するチェック値として部分チェック値を付与し、少なくとも上記部分チェック値を1以上含む部分チェック値集合データ列に対する検証を行なう中間チェック値を検証対象データに付与することを特徴とするデータ検証値付与方法にある。

さらに、本発明のデータ検証値付与方法の一実施態様において、上記部分チェック値は、チェック対象となる部分データをメッセージとし、部分チェック値生成鍵を適用した暗号処理によって生成される値であり、上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとし、総チェック値生成鍵を適用した暗号処理によって生成される値であることを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、上記部分チェック値は、生成する部分チェック値に対応する異なる種類の部分チェック値生成鍵を適用して生成することを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、上記暗号処理はDES暗号処理であることを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、上記部分チェック値は、チェック対象となる部分データをメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であることを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、さらに、上記中間チェック値に対して署名鍵を適用した暗号処理により生成される値をデータ検証のための照合値として適用することを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、データの利用制限態様に応じて異なる署名鍵を上記中間チェック値に対する暗号処理に適用してデータ検証のための照合値とすることを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、上記署名鍵として、データ検証処理を実行するシステムの全エンティティに共通の共通署名鍵と、データ検証処理を実行する各々の装置固有の装置固有署名鍵とをデータの利用制限態様に応じて選択して使用するよう設定することを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッダ部分チェック値と、データの一部を構成するコンテンツ部内データについて生成される1以上のコンテンツチェック値とを含み、上記ヘッダ部分チェック値および上記コンテンツチェック値全てに対する総チェック値を生成してデータ検証を実行するよう設定することを特徴とする。

さらに、本発明のデータ検証値付与方法の一実施態様において、上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッダ部分チェック値を含み、上記1以上のヘッダ部分チェック値および上記データの一部を構成するコンテンツブロックデータからなるデータ列全てに対する総チェック値を生成してデータ検証を実行するよう設定することを特徴とす

る。

さらに、本発明の第6の側面は、データ正当性の検証を実行するデータ検証処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、データを複数部分に分割した部分データを1以上含む部分データ集合に対するチェック値として生成される部分チェック値の照合処理により上記部分データの検証処理を実行するステップと、上記部分チェック値を複数個組み合わせた部分チェック値集合に基づいて生成される中間チェック値を用いて、上記部分チェック値集合を構成する複数の部分チェック値に対応する複数の部分データ集合全体に対する検証処理を実行するステップと、を含むことを特徴とするプログラム提供媒体にある。

さらに、本発明の第7の側面は、データ処理装置において、データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理部と、上記暗号処理に適用する鍵を生成するためのマスター鍵を格納した記憶部とを有し、上記暗号処理部は、上記暗号処理を実行するに必要な個別鍵を、上記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、記憶媒体または通信媒体を介する転送データに関する暗号処理を行なうデータ処理装置であり、上記記憶部は、上記転送データの暗号処理に適用する配送鍵 K_{dis} を生成する配送鍵生成用マスター鍵 MK_{dis} を格納し、上記暗号処理部は、上記記憶部に格納された配送鍵生成用マスター鍵 MK_{dis} と、上記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行して、上記転送データの配送鍵 K_{dis} を生成する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、転送データの転送先あるいは転送元となる外部接続装置の認証処理を行なうデータ処理装置であり、上記記憶部は、上記外部接続装置の認証鍵 K_{ake} を生

成する認証鍵生成用マスター鍵MK a k eを格納し、上記暗号処理部は、上記記憶部に格納された認証鍵生成用マスター鍵MK a k eと、上記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、上記外部接続装置の認証鍵K a k eを生成する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、データに対する署名処理を実行するデータ処理装置であり、上記記憶部は、上記データ処理装置のデータ処理装置署名鍵K d e vを生成する署名鍵生成用マスター鍵MK d e vを格納し、上記暗号処理部は、上記記憶部に格納された署名鍵生成用マスター鍵MK d e vと、上記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、上記データ処理装置のデータ処理装置署名鍵K d e vを生成する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、暗号処理を実行するに必要な個別鍵を、上記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する個別鍵生成処理は、暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、上記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理はDESアルゴリズムを適用した暗号処理であることを特徴とする。

さらに、本発明の第8の側面は、複数のデータ処理装置から構成されるデータ処理システムにおいて、上記複数のデータ処理装置の各々が、データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理に適用する鍵を生成するための共通のマスター鍵を有し、上記複数のデータ処理装置の各々が、上記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて上記暗号処理を実行するに必要な共通の個別鍵を生成する構成を有することを特徴とするデータ処理システムにある。

さらに、本発明のデータ処理システムの一実施態様において、上記複数のデータ処理装置は、コンテンツデータを提供するコンテンツデータ提供装置と、コン

テンツデータの利用を行なうコンテンツデータ利用装置によって構成され、コンテンツデータ提供装置およびコンテンツデータ利用装置の双方が、上記コンテンツデータ提供装置およびコンテンツデータ利用装置間における流通コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵を有し、上記コンテンツデータ提供装置は、上記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、上記コンテンツデータ利用装置は、上記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と上記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、上記コンテンツデータ利用装置は、上記コンテンツデータ提供装置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも1つの配送鍵生成用マスター鍵を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号可能とした構成を有することを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記複数のデータ処理装置の各々に、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するための同一のコンテンツ鍵生成用マスター鍵を格納し、上記複数のデータ処理装置の1つのデータ処理装置Aにおいて、上記コンテンツ鍵生成用マスター鍵と、該データ処理装置Aの装置識別子とに基づいて生成されたコンテンツ鍵により暗号化され記憶媒体に格納されたコンテンツデータを、異なるデータ処理装

置Bにおいて、上記同一のコンテンツ鍵生成用マスター鍵と、上記データ処理装置Aの装置識別子とに基づいてコンテンツ鍵を生成し、該生成したコンテンツ鍵に基づいて、上記データ処理装置Aにおいて上記記憶媒体に格納した暗号化コンテンツデータの復号処理を実行する構成としたことを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、上記複数のデータ処理装置は、ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとによって構成され、上記ホストデバイスおよびスレーブデバイスの双方が、ホストデバイスとスレーブデバイス間の認証処理に適用する認証鍵生成用マスターを有し、上記スレーブデバイスは、上記認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成してスレーブデバイス内メモリに格納し、上記ホストデバイスは、上記認証鍵生成用マスター鍵と、上記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処理を実行する構成を有することを特徴とする。

さらに、本発明の第9の側面は、データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理を実行するデータ処理方法において、暗号処理を実行するに必要な個別鍵を、上記暗号処理に適用する鍵を生成するためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、上記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処理ステップと、を有することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において実行するデータ処理は、記憶媒体または通信媒体を介する転送データに関する暗号処理であり、上記鍵生成ステップは、転送データの暗号処理に適用する配送鍵 K_{dis} を生成する配送鍵生成用マスター鍵 MK_{dis} と、上記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行し、上記転送データの配送鍵 K_{dis} を生成する配送鍵生成ステップであり、上記暗号処理ス

テップは、上記配送鍵生成ステップにおいて生成した配送鍵 K_{dis} に基づいて転送データの暗号処理を実行するステップであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において実行するデータ処理は、転送データの転送先あるいは転送元となる外部接続装置の認証処理であり、上記鍵生成ステップは、上記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成用マスター鍵 MK_{ake} と、上記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、上記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成ステップであり、上記暗号処理ステップは、上記認証鍵生成ステップにおいて生成した認証鍵 K_{ake} に基づいて外部接続装置の認証処理を実行するステップであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理装置において実行するデータ処理は、データに対する署名処理であり、上記鍵生成ステップは、上記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する署名鍵生成用マスター鍵 MK_{dev} と、上記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、上記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する署名鍵生成ステップであり、上記暗号処理ステップは、上記署名鍵生成ステップにおいて生成した署名鍵 K_{dev} に基づいてデータに対する署名処理を実行するステップであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記鍵生成ステップは、暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、上記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記暗号処理はDESアルゴリズムを適用した暗号処理であることを特徴とする。

さらに、本発明の第10の側面は、コンテンツデータを提供するコンテンツデータ提供装置と、コンテンツデータの利用を行なうコンテンツデータ利用装置とからなるデータ処理システムにおけるデータ処理方法であり、上記コンテンツデ

ータ提供装置は、コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、上記コンテンツデータ利用装置は、上記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と上記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、上記コンテンツデータ利用装置は、上記コンテンツデータ提供装置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも1つの配送鍵生成用マスター鍵を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号することを特徴とする。

さらに、本発明の第11の側面は、複数のデータ処理装置によって構成されるデータ処理システムにおけるデータ処理方法であり、上記複数のデータ処理装置中の1つのデータ処理装置Aにおいて、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するためのコンテンツ鍵生成用マスター鍵と、該データ処理装置Aの装置識別子とに基づいて生成されたコンテンツ鍵により暗号化されたコンテンツデータを記憶媒体に格納するステップと、異なるデータ処理装置Bにおいて、上記データ処理装置Aと同一の上記コンテンツ鍵生成用マスター鍵と上記データ処理装置Aの装置識別子とに基づいて上記コンテンツ鍵と同一のコンテンツ鍵を生成するステップと、上記データ処理装置Bにおいて生成したコンテンツ鍵により上記記憶媒体に格納したコンテンツデータの復号を行なうステップと、

を有することを特徴とするデータ処理方法にある。

さらに、本発明の第12の側面は、ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとからなるデータ処理システムにおけるデータ処理方法であり、上記スレーブデバイスは、ホストデバイスとスレーブデバイス間の認証処理に適用する認証鍵を生成するための認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成し、生成した認証鍵を該スレーブデバイス内のメモリに格納し、上記ホストデバイスは、上記認証鍵生成用マスター鍵と、上記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処理を実行することを特徴とするデータ処理方法にある。

さらに、本発明の第13の側面は、データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、暗号処理を実行するに必要な個別鍵を、上記暗号処理に適用する鍵を生成するためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、上記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処理ステップと、を含むことを特徴とするプログラム提供媒体にある。

本発明の第14の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、データ処理装置識別子を格納した記憶部と、コンテンツデータ中に含まれる不正機器リストを抽出し、該リスト内のエントリと上記記憶部に格納された上記データ処理装置識別子との照合処理を実行するリスト検証部と、上記照合処理部における照合処理の結果、上記不正機器リスト中に上記データ処理識別子と一致する情報が含まれる場合において、上記コンテンツデータの再生または記録デバイスに対する格納処理少なくともいずれかの処理の実行を中止する制御部と、を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記リスト検証部は、上記コンテンツデータに対する暗号処理を実行する暗号処理部を有し、上記暗号処理部は、上記コンテンツデータ中に含まれる不正機器リストのチェック値に基づいて上記不正機器リストの改竄の有無を検証し、該検証により、改竄なしと判定した場合にのみ上記照合処理を実行する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、不正機器リストチェック値生成鍵を有し、上記暗号処理部は、検証対象の不正機器リスト構成データに対して上記不正機器リストチェック値生成鍵を適用した暗号処理を実行して不正機器リストチェック値を生成し、該生成した不正機器リストチェック値と、上記コンテンツデータ中に含まれる不正機器リストのチェック値との照合を実行して上記不正機器リストの改竄の有無を検証する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記リスト検証部は、上記コンテンツデータに対する暗号処理を実行する暗号処理部を有し、上記暗号処理部は、上記コンテンツデータ中に含まれる暗号化された不正機器リストの復号処理を実行し、該復号処理の結果として得られた不正機器リストについて上記照合処理を実行する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記リスト検証部は、コンテンツデータの転送先または転送元となる記録デバイスとの相互認証処理を実行する暗号処理部を有し、上記リスト検証部は、上記暗号処理部によって実行される上記記録デバイスとの相互認証処理による認証が成立したことを条件として、上記コンテンツデータ中に含まれる不正機器リストを抽出し上記記憶部に格納された上記データ処理装置識別子との照合処理を実行する構成であることを特徴とする。

さらに、本発明の第15の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法であり、コンテンツデータ中に含まれる不正機器リストを抽出するリスト抽出ステップと、上記リスト抽出ス

テップによって抽出されたリストに含まれるエントリと、データ処理装置内の記憶部に格納された上記データ処理装置識別子との照合処理を実行する照合処理ステップと、上記照合処理ステップにおける照合処理の結果、上記不正機器リスト中に上記データ処理識別子と一致する情報が含まれる場合、上記コンテンツデータの再生または記録デバイスに対する格納処理少なくともいずれかの処理の実行を中止するステップと、を有することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、上記コンテンツデータ中に含まれる不正機器リストのチェック値に基づいて上記不正機器リストの改竄の有無を検証する検証ステップを含み、上記照合処理ステップは、上記検証ステップにより、改竄なしと判定した場合にのみ実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記検証ステップは、検証対象の不正機器リスト構成データに対して不正機器リストチェック値生成鍵を適用した暗号処理を実行して不正機器リストチェック値を生成するステップと、生成した不正機器リストチェック値と、上記コンテンツデータ中に含まれる不正機器リストのチェック値との照合を実行して上記不正機器リストの改竄の有無を検証するステップとを含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、上記コンテンツデータ中に含まれる暗号化された不正機器リストの復号処理を実行する復号ステップを含み、上記照合処理ステップは、上記復号ステップの結果として得られた不正機器リストについて上記照合処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、コンテンツデータの転送先または転送元となる記録デバイスとの相互認証処理ステップを含み、上記照合処理ステップは、上記相互認証処理ステップによって実行される上記記録デバイスとの相互認証処理による認証が成立したことを条件として上記照合処理を実行することを特徴とする。

さらに、本発明の第16の側面は、記憶媒体または通信媒体によって複数の記録再生器に対して提供されるコンテンツデータの生成を行なうコンテンツデータ生成方法であり、コンテンツデータのヘッダ情報として該コンテンツデータの利用の排除対象となる記録再生器の記録再生器識別子を構成データとした不正機器リストを格納してコンテンツデータとすることを特徴とするコンテンツデータ生成方法にある。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、コンテンツデータのヘッダ情報として、上記不正機器リストの改竄チェック用の不正機器リストチェック値を格納することを特徴とする。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、上記不正機器リストを暗号化してコンテンツデータのヘッダ情報中に格納することを特徴とする。

さらに、本発明の第17の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、コンテンツデータ中に含まれる不正機器リストを抽出するリスト抽出ステップと、上記リスト抽出ステップによって抽出されたリストに含まれるエントリと、データ処理装置内の記憶部に格納された上記データ処理装置識別子との照合処理を実行する照合処理ステップと、上記照合処理ステップにおける照合処理の結果、上記不正機器リスト中に上記データ処理識別子と一致する情報が含まれる場合、上記コンテンツデータの再生または記録デバイスに対する格納処理少なくともいずれかの処理の実行を中止するステップと、を有することを特徴とするプログラム提供媒体にある。

さらに、本発明の第18の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、上記コンテンツデータに対する暗号処理を実行する暗号処理部と、上記暗号処理部に対する制御を実行する制御部と、上記暗号処理部における暗号処理に使用され、上記コンテンツ

データを利用する他のデータ処理装置に共通のシステム共通鍵と、上記暗号処理部における暗号処理に使用されるデータ処理装置固有の装置固有鍵または該装置固有鍵を生成するための装置固有識別子の少なくともいずれかを有し、上記暗号処理部は、上記コンテンツデータの利用態様に応じて上記システム共通鍵、または上記装置固有鍵のいずれかを上記コンテンツデータに適用して暗号処理を実行する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、上記コンテンツデータに含まれる利用制限情報に応じて上記システム共通鍵、または上記装置固有鍵のいずれかを上記コンテンツデータに適用して暗号処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、コンテンツデータを記録する記録デバイスを有し、上記暗号処理部は、上記コンテンツデータを自己のデータ処理装置のみにおいて使用する利用制限を付する場合、上記コンテンツデータに対して上記装置固有鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成し、上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能とする場合、上記コンテンツデータに対して上記システム共通鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、データ処理装置固有の署名鍵 K_{dev} 、および複数のデータ処理装置に共通のシステム署名鍵 K_{sys} を有し、上記暗号処理部は、上記コンテンツデータを自己のデータ処理装置のみにおいて使用する利用制限を付して上記記録デバイスに格納する場合、上記コンテンツデータに対して上記装置固有の署名鍵 K_{dev} を適用した暗号処理により装置固有チェック値を生成し、上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能として上記記録デバイスに格納する場合、上記コンテンツデータに対して上記システム署名鍵 K_{sys} を適用した暗号処理により総チェック値を生成し、上記制御部は、上記暗号処理部

の生成した上記装置固有チェック値または上記総チェック値のいずれかを上記コンテンツデータと共に上記記録デバイスに格納する制御を実行することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、データ処理装置固有の署名鍵 K_{dev} 、および複数のデータ処理装置に共通のシステム署名鍵 K_{sys} を有し、上記暗号処理部は、自己のデータ処理装置のみにおいて使用する利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記装置固有の署名鍵 K_{dev} を適用した暗号処理により装置固有チェック値を生成し、該生成した装置固有チェック値の照合処理を実行し、自己のデータ処理装置以外の装置においても使用可能とされた利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記システム署名鍵 K_{sys} を適用した暗号処理により総チェック値を生成し、該生成した総チェック値の照合処理を実行し、上記制御部は、上記装置固有チェック値の照合が成立した場合、あるいは上記総チェック値の照合が成立した場合にのみコンテンツデータの暗号処理部での処理を続行させて再生可能復号データを生成する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、記録データ処理装置署名鍵用マスター鍵 MK_{dev} 、およびデータ処理装置識別子 ID_{dev} を有し、上記暗号処理部は、上記データ処理装置署名鍵用マスター鍵 MK_{dev} と上記データ処理装置識別子 ID_{dev} とに基づく暗号処理によりデータ処理装置固有鍵としての署名鍵 K_{dev} を生成する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、上記データ処理装置識別子 ID_{dev} に対して上記データ処理装置署名鍵用マスター鍵 MK_{dev} を適用したDES暗号処理により上記署名鍵 K_{dev} を生成する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、

上記コンテンツデータに対する暗号処理を実行して中間チェック値を生成し、該中間チェック値に上記データ処理装置固有鍵またはシステム共有鍵を適用した暗号処理を実行することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、上記コンテンツデータを複数部分に分割した部分データを1以上含む部分データ集合に対する暗号処理により部分チェック値を生成し、該生成した部分チェック値を含む部分チェック値集合データ列に対する暗号処理により中間チェック値を生成する構成であることを特徴とする。

さらに、本発明の第19の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法であり、上記コンテンツデータの利用態様に応じて、上記コンテンツデータを利用する他のデータ処理装置に共通の暗号処理用システム共通鍵、または、データ処理装置固有の装置固有鍵のいずれかの暗号処理鍵を選択し、選択した暗号処理鍵を上記コンテンツデータに適用して暗号処理を実行することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、上記暗号処理鍵を選択するステップは、上記コンテンツデータに含まれる利用制限情報に応じて選択するステップであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法におけるコンテンツデータの記録デバイスに対する記録処理において、上記コンテンツデータを自己のデータ処理装置のみにおいて使用する利用制限を付する場合、上記コンテンツデータに対して上記装置固有鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成し、上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能とする場合、上記コンテンツデータに対して上記システム共通鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法におけるコンテンツデータの記録デバイスに対する記録処理において、上記コン

コンテンツデータを自己のデータ処理装置のみににおいて使用する利用制限を付して上記記録デバイスに格納する場合、上記コンテンツデータに対して上記装置固有の署名鍵 K_{dev} を適用した暗号処理により装置固有チェック値を生成し、上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能として上記記録デバイスに格納する場合、上記コンテンツデータに対して上記システム署名鍵 K_{sys} を適用した暗号処理により総チェック値を生成し、上記生成した上記装置固有チェック値または上記総チェック値のいずれかを上記コンテンツデータと共に上記記録デバイスに格納することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法におけるコンテンツデータの再生処理において、自己のデータ処理装置のみににおいて使用する利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記装置固有の署名鍵 K_{dev} を適用した暗号処理により装置固有チェック値を生成し、該生成した装置固有チェック値の照合処理を実行し、自己のデータ処理装置以外の装置においても使用可能とされた利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記システム署名鍵 K_{sys} を適用した暗号処理により総チェック値を生成し、該生成した総チェック値の照合処理を実行し、上記装置固有チェック値の照合が成立した場合、あるいは上記総チェック値の照合が成立した場合にのみコンテンツデータの再生を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、データ処理装置署名鍵用マスター鍵 MK_{dev} とデータ処理装置識別子 ID_{dev} とに基づく暗号処理によりデータ処理装置固有鍵としての署名鍵 K_{dev} を生成するステップを含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記署名鍵 K_{dev} 生成ステップは、上記データ処理装置識別子 ID_{dev} に対して上記データ処理装置署名鍵用マスター鍵 MK_{dev} を適用したDES暗号処理により上記署名鍵 K_{dev} を生成するステップであることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、上記コンテンツデータに対する暗号処理を実行して中間チェック値を生成するステップを含み、上記中間チェック値に上記データ処理装置固有鍵またはシステム共有鍵を適用した暗号処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、上記コンテンツデータを複数部分に分割した部分データを1以上含む部分データ集合に対する暗号処理により部分チェック値を生成し、該生成した部分チェック値を含む部分チェック値集合データ列に対する暗号処理により中間チェック値を生成することを特徴とする。

さらに、本発明の第20の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、上記コンテンツデータの利用態様に応じて、上記コンテンツデータを利用する他のデータ処理装置に共通の暗号処理用システム共通鍵、または、データ処理装置固有の装置固有鍵のいずれかの暗号処理鍵を選択するステップと、選択した暗号処理鍵を上記コンテンツデータに適用して暗号処理を実行するステップと、を含むことを特徴とするプログラム提供媒体にある。

さらに、本発明の第21の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、上記コンテンツデータに対する暗号処理を実行する暗号処理部と、上記暗号処理部に対する制御を実行する制御部とを有し、上記暗号処理部は、データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位の正当性検証処理を実行する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置

は、コンテンツチェック値生成鍵を有し、上記暗号処理部は、検証対象のコンテンツブロックデータに基づいてコンテンツ中間値を生成し、該コンテンツ中間値に対する上記コンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、検証対象のコンテンツブロックデータが暗号化されている場合、該コンテンツブロックデータの復号処理によって得られる復号文全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成し、検証対象のコンテンツブロックデータが暗号化されていない場合、コンテンツブロックデータ全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部における上記中間チェック値の生成処理において適用する上記所定の演算処理は排他的論理和演算であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、CBCモードによる暗号処理構成を有し、検証対象のコンテンツブロックデータが暗号化されている場合のコンテンツ中間値生成処理に適用する上記復号処理は、CBCモードによる復号処理であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部の有するCBCモードによる暗号処理構成は、処理対象となるメッセージ列の一部においてのみ複数回共通鍵暗号処理が適用される構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、コンテンツブロックデータに複数のパーツが含まれ、該コンテンツブロックデータに含まれる一部のパーツが検証対象である場合において、検証対象パーツに基づいてコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位毎の正当性検証処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが1つである場合において、上記要検証パーツが暗号化されている場合、要検証パーツの復号処理によって得られる復号文全体を所定バイト単位で排他論理和した値に、コンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成し、上記要検証パーツが暗号化されていない場合、該要検証パーツ全体を所定バイト単位で排他論理和した値を、上記コンテンツチェック値生成鍵を適用して暗号処理を実行してコンテンツチェック値を生成する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部は、上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが複数である場合において、各パーツ毎にコンテンツチェック値生成鍵を適用して暗号処理を実行して得られたパーツチェック値の連結データに対して、さらに上記コンテンツチェック値生成鍵を適用した暗号処理を実行して得られる結果をコンテンツチェック値とする構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、上記暗号処理部において正当性検証の実行されたコンテンツブロックデータを含むコンテンツデータを格納する記録デバイスを有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記暗号処理部におけるコンテンツチェック値の照合処理において、照合が成立しなかった場合において、上記制御部は、上記記録デバイスへの格納処理を中止する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、上記暗号処理部において正当性検証の実行されたデータを再生する再生処理部を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置

は、上記暗号処理部におけるコンテンツチェック値の照合処理において、照合が成立しなかった場合において、上記制御部は、上記再生処理部での再生処理を中止する構成を有することを特徴とする。

さらに、本発明の第22の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法であり、データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位の正当性検証処理を実行することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、検証対象のコンテンツブロックデータに基づいてコンテンツ中間値を生成し、生成したコンテンツ中間値に対するコンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、検証対象のコンテンツブロックデータが暗号化されている場合、該コンテンツブロックデータの復号処理によって得られる復号文全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成し、検証対象のコンテンツブロックデータが暗号化されていない場合、コンテンツブロックデータ全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、上記中間チェック値の生成処理において適用する上記所定の演算処理は排他的論理和演算であることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記コンテンツ中間値の生成処理において、検証対象のコンテンツブロックデータが暗号化されている場合のコンテンツ中間値生成処理に適用する上記復号処理は、CBCモードによる復号処理であることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記CBCモードによる復号処理構成は、処理対象となるメッセージ列の一部においてのみ複数回共通鍵暗号処理が適用することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、コンテンツブロックデータに複数のパーツが含まれ、該コンテンツブロックデータに含まれる一部のパーツが検証対象である場合、検証対象パーツに基づいてコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位毎の正当性検証処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが1つである場合、上記要検証パーツが暗号化されている場合、要検証パーツの復号処理によって得られる復号文全体を所定バイト単位で排他論理和した値に、コンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成し、上記要検証パーツが暗号化されていない場合、該要検証パーツ全体を所定バイト単位で排他論理和した値を、上記コンテンツチェック値生成鍵を適用して暗号処理を実行してコンテンツチェック値を生成することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法において、上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが複数である場合、各パーツ毎にコンテンツチェック値生成鍵を適用して暗号処理を実行して得られたパーツチェック値の連結データに対して、さらに上記コンテンツチェック値生成鍵を適用した暗号処理を実行して得られる結果をコンテンツチェック値とすることを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、正当性検証の実行されたコンテンツブロックデータを含むコンテンツデータを格納するステップを含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、コンテンツチェック値の照合処理において、照合が成立しなかった場合において、上記制御部は、上記記録デバイスへの格納処理を中止することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、正当性検証の実行されたデータを再生する再生処理を実行するステップを含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、コンテンツチェック値の照合処理において、照合が成立しなかった場合において、再生処理を中止することを特徴とする。

さらに、本発明の第23の側面は、コンテンツデータ検証処理のためのコンテンツデータ検証値付与方法であり、データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成し、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とするコンテンツデータ検証値付与方法にある。

さらに、本発明のコンテンツデータ検証値付与方法の一実施態様において、上記コンテンツチェック値は、チェック対象となるコンテンツブロックデータをメッセージとし、コンテンツチェック値生成鍵を適用した暗号処理によって生成される値であることを特徴とする。

さらに、本発明のコンテンツデータ検証値付与方法の一実施態様において、上記コンテンツチェック値は、検証対象のコンテンツブロックデータに基づいてコンテンツ中間値を生成し、該コンテンツ中間値に対する上記コンテンツチェック値生成鍵を適用した暗号処理を実行して生成される値であることを特徴とする。

さらに、本発明のコンテンツデータ検証値付与方法の一実施態様において、上記コンテンツチェック値は、検証対象のコンテンツブロックデータに対するCBCモードによる暗号処理を実行することによって生成される値であることを特徴とする。

さらに、本発明のコンテンツデータ検証値付与方法の一実施態様において、上記CBCモードによる暗号処理構成は、処理対象となるメッセージ列の一部においてのみ複数回共通鍵暗号処理が適用される構成であることを特徴とする。

さらに、本発明のコンテンツデータ検証値付与方法の一実施態様において、コンテンツブロックデータに複数のパーツが含まれ、該コンテンツブロックデータに含まれる一部のパーツを検証対象とする場合において、検証対象パーツに基づいてコンテンツチェック値を生成し、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とする。

さらに、本発明のコンテンツデータ検証値付与方法の一実施態様において、上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが1つである場合において、上記要検証パーツが暗号化されている場合、要検証パーツの復号処理によって得られる復号文全体を所定バイト単位で排他論理和した値に、コンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成し、上記要検証パーツが暗号化されていない場合、該要検証パーツ全体を所定バイト単位で排他論理和した値を、上記コンテンツチェック値生成鍵を適用して暗号処理を実行してコンテンツチェック値を生成し、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とする。

さらに、本発明のコンテンツデータ検証値付与方法の一実施態様において、上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが複数である場合において、各パーツ毎にコンテンツチェック値生成鍵を適用して暗号処理を実行して得られたパーツチェック値の連結データに対して、さらに上記コンテンツチェック値生成鍵を適用した暗号処理を実行して得られる結果をコンテンツチェック値とし、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とする。

さらに、本発明の第24の側面は、記憶媒体または通信媒体によって提供され

るコンテンツデータの処理を行なうデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成するステップと、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位の正当性検証処理を実行するステップと、を含むことを特徴とするプログラム提供媒体にある。

さらに、本発明の第25の側面は、少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データを生成する処理を実行するデータ処理装置であり、上記データ処理装置は、上記記録デバイスに対する格納対象となるコンテンツデータが、上記コンテンツブロックの暗号鍵 K_{con} を暗号鍵 K_{dis} によって暗号処理した暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部に格納したデータによって構成されている場合において、上記暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部から取り出して復号処理を実行して復号データ K_{con} を生成し、該生成した復号データ K_{con} に対して異なる暗号鍵 K_{str} を適用して暗号処理を実行することにより、暗号鍵 K_{str} によって暗号処理された新たな暗号鍵データ $K_{str}[K_{con}]$ を生成して上記コンテンツデータのヘッダ部に格納する処理を実行する構成を有することを特徴とするデータ処理装置にある。

本発明の第26の側面は、少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データを生成する処理を実行するデータ処理装置であり、上記データ処理装置は、上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵 K_{blc} によって暗号化されたコンテンツと、暗号鍵 K_{con} によって暗号化された暗号鍵データ $K_{con}[K_{blc}]$ によって構成され、さらに、暗号鍵 K

c o n を暗号鍵 K d i s によって暗号処理した暗号鍵データ K d i s [K c o n] を上記ヘッダ部に格納した構成を有する場合において、上記暗号鍵データ K d i s [K c o n] を上記ヘッダ部から取り出して復号処理を実行して復号データ K c o n を生成し、該生成した復号データ K c o n に対して異なる暗号鍵 K s t r を適用して暗号処理を実行することにより、暗号鍵 K s t r によって暗号処理された暗号鍵データ K s t r [K c o n] を生成して上記コンテンツデータのヘッダ部に格納する処理を実行する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明の第 27 の側面は、少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データを生成する処理を実行するデータ処理装置であり、上記データ処理装置は、上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵 K b l c によって暗号化されたコンテンツと、暗号鍵 K d i s によって暗号化された暗号鍵データ K d i s [K b l c] によって構成されている場合において、上記暗号鍵データ K d i s [K b l c] を上記コンテンツブロック部から取り出して、該暗号鍵 K b l c の復号処理を実行して復号データ K b l c を生成し、該生成した復号データ K b l c に対して異なる暗号鍵 K s t r を適用して暗号処理を実行することにより、暗号鍵 K s t r によって暗号処理された暗号鍵 K s t r [K b l c] を生成してコンテンツブロック部に格納する処理を実行する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明の第 28 の側面は、コンテンツデータを生成するコンテンツデータ生成方法であり、音声情報、画像情報、プログラムデータの少なくともいずれかを含むデータによって構成されるコンテンツブロックを複数ブロック連結し、複数のコンテンツブロックに含まれる少なくとも一部のコンテンツブロックを暗号鍵 K c o n によって暗号処理し、上記暗号鍵 K c o n を暗号鍵 K d i s によって暗号処理した暗号鍵データ K d i s [K c o n] を生成して上記コンテンツ

データのヘッダ部に格納し、複数のコンテンツブロックとヘッダ部を含むコンテンツデータを生成するコンテンツデータ生成方法にある。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、さらに、コンテンツデータの識別情報、コンテンツデータのデータ長、コンテンツデータのデータ種類を含む取扱方針情報、上記コンテンツブロックのデータ長、暗号処理の有無を含む情報を格納したブロック情報を生成して、上記ヘッダ部に格納する処理を含むことを特徴とする。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、上記コンテンツデータ生成方法は、さらに、上記ヘッダ部を構成する一部の情報に基づく部分チェック値を生成して、該部分チェック値を上記ヘッダ部に格納し、さらに、上記部分チェック値に基づく総チェック値を生成して、該総チェック値を上記ヘッダ部に格納する処理を含むことを特徴とする。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、上記部分チェック値の生成処理および総チェック値の生成処理は、チェック対象となるデータをメッセージとし、チェック値生成鍵を暗号鍵とするDES暗号処理アルゴリズムを適用して実行することを特徴とする。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、上記コンテンツデータ生成方法は、さらに、上記ブロック情報を暗号鍵K b i tにより暗号化処理し、該暗号鍵K b i tを暗号鍵K d i sによって生成した暗号鍵データK d i s [K b i t]を上記ヘッダ部に格納することを特徴とする。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、上記コンテンツブロック中の複数ブロックの各々のブロックは共通する一定のデータ長として生成することを特徴とする。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、上記コンテンツブロック中の複数ブロックの各々のブロックは暗号データ部と非暗号データ部とを規則的に配列した構成として生成することを特徴とする。

さらに、本発明の第29の側面は、コンテンツデータを生成するコンテンツデ

ータ生成方法であり、音声情報、画像情報、プログラムデータの少なくともいずれかを含むコンテンツブロックを複数ブロック連結するとともに、複数のコンテンツブロックの少なくとも一部のブロックを、音声情報、画像情報、プログラムデータの少なくともいずれかを含むデータを暗号鍵K b l cで暗号化した暗号データ部と、該暗号データ部の暗号鍵K b l cを暗号鍵K c o nによって暗号処理した暗号鍵データK c o n [K b l c]の組によって構成し、上記暗号鍵K c o nを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K c o n]を生成して上記コンテンツデータのヘッダ部に格納し、複数のコンテンツブロックとヘッダ部を含むコンテンツデータを生成するコンテンツデータ生成方法にある。

さらに、本発明の第30の側面は、コンテンツデータを生成するコンテンツデータ生成方法であり、音声情報、画像情報、プログラムデータの少なくともいずれかを含むコンテンツブロックを複数ブロック連結するとともに、複数のコンテンツブロックの少なくとも一部のブロックを、音声情報、画像情報、プログラムデータの少なくともいずれかを含むデータを暗号鍵K b l cで暗号化した暗号データ部と、該暗号データ部の暗号鍵K b l cを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K b l c]の組によって構成し、複数のコンテンツブロックとヘッダ部を含むコンテンツデータを生成するコンテンツデータ生成方法にある。

さらに、本発明の第31の側面は、少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納処理を実行するデータ処理方法であり、上記記録デバイスに対する格納対象となるコンテンツデータが、上記コンテンツブロックの暗号鍵K c o nを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K c o n]を上記ヘッダ部に格納したデータによって構成されている場合において、上記暗号鍵データK d i s [K c o n]を上記ヘッダ部から取り出して復号処理を実行して復号データK c o nを生成し、

該生成した復号データ K_{con} に対して異なる暗号鍵 K_{str} を適用して暗号処理を実行することにより、暗号鍵 K_{str} によって暗号処理された新たな暗号鍵データ $K_{str}[K_{con}]$ を生成し、上記生成した暗号鍵データ $K_{str}[K_{con}]$ を上記コンテンツデータのヘッダ部に格納し、上記複数のコンテンツブロックと共に上記記録デバイスに格納することを特徴とするデータ処理方法にある。

さらに、本発明の第32の側面は、少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納処理を実行するデータ処理方法であり、上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵 K_{blc} によって暗号化されたコンテンツと、暗号鍵 K_{con} によって暗号化された暗号鍵データ $K_{con}[K_{blc}]$ によって構成され、さらに、暗号鍵 K_{con} を暗号鍵 K_{dis} によって暗号処理した暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部に格納した構成を有する場合において、上記暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部から取り出して復号処理を実行して復号データ K_{con} を生成し、該生成した復号データ K_{con} に対して異なる暗号鍵 K_{str} を適用して暗号処理を実行することにより、暗号鍵 K_{str} によって暗号処理された暗号鍵データ $K_{str}[K_{con}]$ を生成し、上記生成した暗号鍵データ $K_{str}[K_{con}]$ を上記コンテンツデータのヘッダ部に格納し、上記複数のコンテンツブロックと共に上記記録デバイスに格納することを特徴とするデータ処理方法にある。

さらに、本発明の第33の側面は、少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納処理を実行するデータ処理方法であり、上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵 K_{blc} によって暗号化されたコンテンツと、暗号鍵 K_{dis} によって暗号化された暗号鍵データ $K_{dis}[K_{con}]$ を生成し、上記生成した暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部に格納し、上記複数のコンテンツブロックと共に上記記録デバイスに格納することを特徴とするデータ処理方法にある。

b l c] によって構成されている場合において、上記暗号鍵データ K d i s [K b l c] を上記コンテンツブロック部から取り出して、該暗号鍵 K b l c の復号処理を実行して復号データ K b l c を生成し、該生成した復号データ K b l c に対して異なる暗号鍵 K s t r を適用して暗号処理を実行することにより、暗号鍵 K s t r によって暗号処理された暗号鍵 K s t r [K b l c] を生成し、該生成した暗号鍵 K s t r [K b l c] をコンテンツブロック部に格納し、複数のコンテンツブロックと共に上記記録デバイスに格納することを特徴とするデータ処理方法にある。

さらに、本発明の第 3 4 の側面は、少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データの生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、上記記録デバイスに対する格納対象となるコンテンツデータが、上記コンテンツブロックの暗号鍵 K c o n を暗号鍵 K d i s によって暗号処理した暗号鍵データ K d i s [K c o n] を上記ヘッダ部に格納したデータによって構成されている場合において、上記暗号鍵データ K d i s [K c o n] を上記ヘッダ部から取り出して復号処理を実行して復号データ K c o n を生成するステップと、該生成した復号データ K c o n に対して異なる暗号鍵 K s t r を適用して暗号処理を実行することにより、暗号鍵 K s t r によって暗号処理された新たな暗号鍵データ K s t r [K c o n] を生成するステップと、上記生成した暗号鍵データ K s t r [K c o n] を上記コンテンツデータのヘッダ部に格納するステップと、を含むことを特徴とするプログラム提供媒体にある。

本発明の第 3 5 の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理を行なうデータ処理装置であり、圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを含むコンテンツデータのコンテンツデータ解析を実行し、該コンテンツデータから圧縮コンテンツと、伸長処理プロ

グラムの抽出処理を実行するコンテンツデータ解析部と、上記コンテンツデータ解析部の解析結果として得られたコンテンツデータに含まれる伸長処理プログラムを用いて該コンテンツデータに含まれる圧縮コンテンツの伸長処理を実行する伸長処理部とを有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記コンテンツデータ解析部によって抽出された圧縮コンテンツを格納するデータ記憶部と、上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶部とを有し、上記伸長処理部は、上記データ記憶部に記憶された圧縮コンテンツに対して、上記プログラム記憶部に記憶された伸長処理プログラムを適用して伸長処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記コンテンツデータ解析部は、上記コンテンツデータに含まれるヘッダ情報に基づいてコンテンツデータの構成情報を取得してコンテンツデータの解析を行なう構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記ヘッダ情報には、圧縮コンテンツの再生優先順位情報が含まれ、上記伸長処理部において伸長処理対象となる圧縮コンテンツが複数ある場合、上記伸長処理部は、上記コンテンツデータ解析部において取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次コンテンツ伸長処理を実行する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、伸長処理対象となる圧縮コンテンツの情報を表示する表示手段と、上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力手段を有し、上記伸長処理部は、上記入力手段から入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行する構成であることを特徴とする。

さらに、本発明の第36の側面は、記憶媒体または通信媒体によって提供され

るコンテンツデータの再生処理を行なうデータ処理装置であり、圧縮コンテンツ、または伸長処理プログラムのいずれかを含むコンテンツデータを受領し、受領コンテンツデータに含まれるヘッダ情報から該コンテンツデータが圧縮コンテンツであるか伸長処理プログラムであるかを判別するとともに、該コンテンツデータが圧縮コンテンツである場合、該コンテンツデータのヘッダ情報から、該圧縮コンテンツに適用された圧縮処理プログラム種類を取得し、該コンテンツデータが伸長処理プログラムである場合、該コンテンツデータのヘッダ情報から伸長処理プログラム種類を取得するコンテンツデータ解析部と、圧縮コンテンツの伸長処理を実行する伸長処理部とを有し、上記伸長処理部は、上記コンテンツデータ解析部が解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、上記コンテンツデータ解析部によって解析された伸長処理プログラム種類に基づいて選択し、該選択した伸長処理プログラムによる伸長処理を実行する構成を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、上記コンテンツデータ解析部によって抽出された圧縮コンテンツを格納するデータ記憶部と、上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶部とを有し、上記伸長処理部は、上記データ記憶部に記憶された圧縮コンテンツに対して、上記プログラム記憶部に記憶された伸長処理プログラムを適用して伸長処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記ヘッダ情報には、圧縮コンテンツの再生優先順位情報が含まれ、伸長処理対象となる圧縮コンテンツが複数ある場合、上記伸長処理部におけるコンテンツ伸長処理は、上記コンテンツデータ解析部において取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次実行する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、伸長処理プログラムを検索する検索手段を有し、上記検索手段は、上記コン

テンツデータ解析部が解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、上記データ処理装置がアクセス可能なプログラム格納手段を検索対象として検索する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、上記データ処理装置は、さらに、伸長処理対象となる圧縮コンテンツの情報を表示する表示手段と、上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力手段を有し、上記伸長処理部は、上記入力手段から入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行する構成であることを特徴とする。

さらに、本発明の第37の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理を行なうデータ処理方法であり、圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを含むコンテンツデータのコンテンツデータ解析を実行し、該コンテンツデータから圧縮コンテンツと、伸長処理プログラムの抽出処理を実行するコンテンツデータ解析ステップと、上記コンテンツデータ解析ステップの解析結果として得られたコンテンツデータに含まれる伸長処理プログラムを用いて該コンテンツデータに含まれる圧縮コンテンツの伸長処理を実行する伸長処理ステップとを有することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、上記コンテンツデータ解析ステップによって抽出された圧縮コンテンツを格納するデータ記憶ステップと、上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶ステップとを有し、上記伸長処理ステップは、上記データ記憶ステップにおいて記憶された圧縮コンテンツに対して、上記プログラム記憶ステップにおいて記憶された伸長処理プログラムを適用して伸長処理を実行する構成を有することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記コンテンツデータ解析ステップは、上記コンテンツデータに含まれるヘッダ情報に基づいてコン

テンツデータの構成情報を取得してコンテンツデータの解析を行なうことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記ヘッダ情報には、圧縮コンテンツの再生優先順位情報が含まれ、上記伸長処理部において伸長処理対象となる圧縮コンテンツが複数ある場合、上記伸長処理ステップは、上記コンテンツデータ解析ステップにおいて取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次コンテンツ伸長処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、伸長処理対象となる圧縮コンテンツの情報を表示手段に表示する表示ステップと、上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力ステップとを有し、上記伸長処理ステップは、上記入力ステップにおいて入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行することを特徴とする。

さらに、本発明の第38の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理を行なうデータ処理方法であり、圧縮コンテンツ、または伸長処理プログラムのいずれかを含むコンテンツデータを受領し、受領コンテンツデータに含まれるヘッダ情報から該コンテンツデータが圧縮コンテンツであるか伸長処理プログラムであるかを判別するとともに、該コンテンツデータが圧縮コンテンツである場合、該コンテンツデータのヘッダ情報から、該圧縮コンテンツに適用された圧縮処理プログラム種類を取得し、該コンテンツデータが伸長処理プログラムである場合、該コンテンツデータのヘッダ情報から伸長処理プログラム種類を取得するコンテンツデータ解析ステップと、上記コンテンツデータ解析ステップにおいて解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、上記コンテンツデータ解析ステップによって解析された伸長処理プログラム種類に基づいて選択する選択ステップと

、上記選択ステップにおいて選択した伸長処理プログラムによる伸長処理を実行する伸長処理ステップとを有することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、上記コンテンツデータ解析部によって抽出された圧縮コンテンツを格納するデータ記憶ステップと、上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶ステップとを有し、上記伸長処理ステップは、上記データ記憶ステップにおいて記憶された圧縮コンテンツに対して、上記プログラム記憶ステップにおいて記憶された伸長処理プログラムを適用して伸長処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記ヘッダ情報には、圧縮コンテンツの再生優先順位情報が含まれ、伸長処理対象となる圧縮コンテンツが複数ある場合、上記伸長処理ステップは、上記コンテンツデータ解析ステップにおいて取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、伸長処理プログラムを検索する検索ステップを有し、上記検索ステップは、上記コンテンツデータ解析ステップにおいて解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、アクセス可能なプログラム格納手段を検索対象として検索することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、上記データ処理方法は、さらに、伸長処理対象となる圧縮コンテンツの情報を表示手段に表示する表示ステップと、上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力ステップとを有し、上記伸長処理ステップは、上記入力手段から入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行することを特徴とする。

さらに、本発明の第39の側面は、記憶媒体または通信媒体によって提供する

コンテンツデータの生成処理を行なうコンテンツデータ生成方法であり、圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを組み合わせたコンテンツデータを生成することを特徴とするコンテンツデータ生成方法にある。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、さらに、上記コンテンツデータのヘッダ情報として該コンテンツデータの構成情報を付加することを特徴とする。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、さらに、上記コンテンツデータのヘッダ情報として、該コンテンツデータに含まれるコンテンツの再生優先順位情報を付加することを特徴とする。

さらに、本発明の第40の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの生成処理を行なうコンテンツデータ生成方法であり、コンテンツデータが圧縮コンテンツであるか伸長処理プログラムであるかを識別するコンテンツデータ種類をヘッダ情報として付加し、該コンテンツデータが圧縮コンテンツである場合は、該圧縮コンテンツに適用された圧縮処理プログラム種類をヘッダ情報として付加し、該コンテンツデータが伸長処理プログラムである場合は、伸長処理プログラム種類をヘッダ情報として付加したコンテンツデータを生成することを特徴とするコンテンツデータ生成方法にある。

さらに、本発明のコンテンツデータ生成方法の一実施態様において、上記コンテンツデータのヘッダ情報として、該コンテンツデータに含まれるコンテンツの再生優先順位情報を付加することを特徴とする。

さらに、本発明の第41の側面は、記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを含むコンテンツデータのコンテンツデータ解析を実行し、該コンテンツデータから圧縮コンテンツと、伸長処理プログラムの抽出処理を実行するコンテンツデータ解析ステップと、上記コンテンツデータ解析ステップの解析結果とし

て得られたコンテンツデータに含まれる伸長処理プログラムを用いて該コンテンツデータに含まれる圧縮コンテンツの伸長処理を実行する伸長処理ステップとを有することを特徴とするプログラム提供媒体にある。

本発明に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

このように、本発明のデータ処理装置およびデータ処理方法によれば、コンテンツデータを複数部分に分割した部分データを1以上含む部分データ集合に対するチェック値として生成される部分チェック値の照合処理により部分データの検証処理を実行し、部分チェック値を複数個組み合わせた部分チェック値集合に対する検証を行なう部分チェック値検証用チェック値の照合処理により、部分チェック値集合を構成する複数の部分チェック値に対応する複数の部分データ集合全体に対する検証処理を実行する構成としたので、コンテンツデータ全体に対する唯一のチェック値を付与した構成と異なり、部分的な検証処理が可能となり、また、全体の検証処理も、部分チェック値を使用して実行するので、効率的となる。

さらに、本発明のデータ処理装置およびデータ処理方法によれば、改竄の恐れ

のないデータ部分に対する検証処理を省略する等、コンテンツデータの使用態様、例えばダウンロード処理、再生処理に応じた検証処理が可能となり、使用態様に則した効率的な検証を行なうことができる。

さらに、本発明のデータ処理装置およびデータ処理方法によれば、データ暗号化、データ復号化、データ検証、認証処理、署名処理等の暗号処理を実行するために必要となる個別鍵を記憶部に格納せず、これらの個別鍵を生成するためのマスター鍵を記憶部に格納した構成を持ち、データ処理装置における暗号処理部が、暗号鍵、認証鍵等の個別鍵を必要に応じて、それらの個別鍵に対応するマスター鍵を記憶部から取り出して、取り出したマスター鍵と、装置またはデータの識別データに基づいて、例えばDESアルゴリズムを適用した暗号処理を実行して、暗号鍵、認証鍵等の個別鍵を生成する構成としたので、個別鍵自体が記憶部から漏洩する可能性がなく、個別鍵を得るためには、個別鍵生成アルゴリズムと、マスター鍵の双方の情報、さらに装置またはデータの識別データ等、複数の情報が必要となり、暗号処理システムのセキュリティを高めることが可能となる。また、個別鍵が何らかの理由により漏洩したした場合でも、その被害の範囲は個別鍵の範囲に限定されるため、システム前名対の崩壊にはつながらないといえる。

さらに、本発明のデータ処理装置およびデータ処理方法によれば、装置またはデータの識別データに基づいて、個別鍵を逐次生成する構成であるので、個々の装置に適用する鍵のリストを管理装置において保持する必要がなく、セキュリティが高まると同時にシステム管理も容易になる。

さらに、本発明のデータ処理装置、データ処理方法およびコンテンツデータ生成方法によれば、コンテンツデータに不正機器の識別データ情報を格納し、記録再生器におけるコンテンツ利用に先立って、不正機器リストと、コンテンツを利用しようとする記録再生器の記録再生器識別子との照合処理を実行して、照合の結果、不正機器リストに含まれるエントリに記録再生器識別子と一致するエントリが存在した場合には、以降の処理、例えばコンテンツデータ復号、ダウンロード、再生処理等の実行を中止する構成としたので不正に鍵を取得した再生機器等

によるコンテンツの不正利用を排除することが可能となる。

さらに、本発明のデータ処理装置、データ処理方法およびコンテンツデータ生成方法によれば、コンテンツデータ中の不正機器リスト用のチェック値を併せてコンテンツデータに含ませる構成としたので、リスト自体の改竄の防止が図れ、さらにセキュリティの高いコンテンツデータ利用構成が提供可能となる。

さらに、本発明のデータ処理装置およびデータ処理方法によれば、記録再生器、PC等のデータ処理装置にデータ処理装置固有の装置固有鍵と、コンテンツデータを利用する他のデータ処理装置に共通のシステム共通鍵とを格納したのでコンテンツの利用制限に応じたコンテンツ処理が可能となる。データ処理装置は、これら2つの鍵をコンテンツの利用制限に応じて選択的に利用する。例えばそのデータ処理装置においてのみ利用可能なコンテンツである場合は、データ処理装置固有の鍵を用い、一方、他のシステムにおいても利用可能なコンテンツである場合にはシステム共通鍵を用いてコンテンツデータのチェック値生成、照合処理を実行する。照合が成立した場合にのみ暗号化データを復号して再生することが可能となるので、そのデータ処理装置のみが利用可能なコンテンツ、あるいはシステムに共通して利用可能なコンテンツ等、コンテンツの利用制限に応じた処理が可能となる。

さらに、本発明のデータ処理装置、データ処理方法およびコンテンツデータ検証値付与方法によれば、コンテンツブロックデータ単位にコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行し、さらに、検証対象のコンテンツブロックデータに基づいてコンテンツ中間値を生成してコンテンツチェック値生成鍵を適用した暗号処理によりコンテンツチェック値を生成する構成としたので、従来のデータ全体の処理に比較して効率的な検証が可能となる。

さらに、本発明のデータ処理装置、データ処理方法およびコンテンツデータ検証値付与方法によれば、コンテンツブロック単位での検証が可能となるとともに、コンテンツデータの使用態様、例えばダウンロード処理、再生処理に応じた簡

略化した検証処理が可能となり、使用態様に則した効率的な検証を行なうことができる。

さらに、本発明のデータ処理装置、コンテンツデータ生成方法、およびデータ処理方法においては、コンテンツデータ中に複数のコンテンツブロックを設け、各コンテンツブロック単位での暗号化処理を可能とした構成を持ち、またコンテンツ暗号化に用いた鍵をさらに暗号化してヘッダ部に格納する構成としたので、例えば複数のコンテンツブロックが存在し、暗号処理の必要なブロックと、不要なブロックとが混在する場合でも、各ブロックを連結した任意なデータ構成とすることが可能となる。

さらに、本発明のデータ処理装置、データ処理システム、およびデータ処理方法によれば、コンテンツブロックの構成を規則的構成、例えば一律のデータ長を持つ構成、あるいは暗号化ブロックと非暗号化（平文）ブロックとを交互に配置した構成とすることにより、その復号処理等を速やかに実行することが可能となり、コンテンツデータの内容に応じた処理、例えば音楽データの再生等に適した暗号化コンテンツデータの提供が可能となる。

さらに、本発明のデータ処理装置、データ処理方法およびコンテンツデータ生成方法は、コンテンツが圧縮された音声データ、あるいは画像データ等である場合の再生処理を効率的に実行することができる。すなわち、コンテンツデータの構成を圧縮データと伸長処理プログラムとを組み合わせた構成とすることで、再生処理装置において、圧縮コンテンツデータに付帯する伸長処理プログラムを適用した伸長処理が可能となり、再生処理装置内に伸長処理プログラムが存在せず再生ができないという事態が回避できる。

さらに、本発明のデータ処理装置、データ処理方法およびコンテンツデータ生成方法によれば、コンテンツデータの構成を圧縮データとその圧縮処理プログラム種類を格納したヘッダ部の組み合わせとし、また、コンテンツが伸長処理プログラムである場合、コンテンツデータを伸長処理プログラムとそのプログラム種類を格納したヘッダ部の組み合わせとすることにより、再生処理装置が、圧縮コン

コンテンツデータに適用可能な伸長処理プログラムをヘッダ情報に基づいて判定し、さらに再生処理装置がアクセス可能な記録デバイス等から適用可能なプログラムを検索して伸長処理を実行する構成としたので、ユーザによるプログラム検索処理を実行する必要がなくなり、効率的な再生処理が可能となる。

図面の簡単な説明

図 1 は、従来のデータ処理システムの構成を示す図である。

図 2 は、本発明の適用されるデータ処理装置の構成を示す図である。

図 3 は、本発明の適用されるデータ処理装置の構成を示す図である。

図 4 は、メディア上、通信路上におけるコンテンツデータのデータフォーマットを示す図である。

図 5 は、コンテンツデータ中のヘッダに含まれる取扱方針を示す図である。

図 6 は、コンテンツデータ中のヘッダに含まれるブロック情報を示す図である。

図 7 は、DES を用いた電子署名生成方法を示す図である。

図 8 は、トリプルDES を用いた電子署名生成方法を示す図である。

図 9 は、トリプルDES の態様を説明する図である。

図 10 は、一部にトリプルDES を用いた電子署名生成方法を示す図である。

図 11 は、電子署名生成における処理フローを示す図である。

図 12 は、電子署名検証における処理フローを示す図である。

図 13 は、対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

図 14 は、公開鍵証明書を説明する図である。

図 15 は、非対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

図 16 は、楕円曲線暗号を用いた暗号化処理の処理フローを示す図である。

図 17 は、楕円曲線暗号を用いた復号化処理の処理フローを示す図である。

図 1 8 は、記録再生器上のデータ保持状況を示す図である。

図 1 9 は、記録デバイス上のデータ保持状況を示す図である。

図 2 0 は、記録再生器と記録デバイスとの相互認証処理フローを示す図である。

図 2 1 は、記録再生器のマスタ鍵と記録デバイスの対応鍵ブロックとの関係を示す図である。

図 2 2 は、コンテンツのダウンロード処理における処理フローを示す図である。

図 2 3 は、チェック値 A : I C V a の生成方法を説明する図である。

図 2 4 は、チェック値 B : I C V b の生成方法を説明する図である。

図 2 5 は、総チェック値、記録再生器固有チェック値の生成方法を説明する図である。

図 2 6 は、記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報 = 0）を示す図である。

図 2 7 は、記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報 = 1）を示す図である。

図 2 8 は、コンテンツの再生処理における処理フローを示す図である。

図 2 9 は、記録デバイスにおけるコマンド実行方法について説明する図である。

図 3 0 は、記録デバイスにおけるコンテンツ格納処理におけるコマンド実行方法について説明する図である。

図 3 1 は、記録デバイスにおけるコンテンツ再生処理におけるコマンド実行方法について説明する図である。

図 3 2 は、コンテンツデータフォーマットのフォーマット・タイプ 0 の構成を説明する図である。

図 3 3 は、コンテンツデータフォーマットのフォーマット・タイプ 1 の構成を説明する図である。

図34は、コンテンツデータフォーマットのフォーマット・タイプ2の構成を説明する図である。

図35は、コンテンツデータフォーマットのフォーマット・タイプ3の構成を説明する図である。

図36は、フォーマット・タイプ0におけるコンテンツチェック値ICV_iの生成処理方法を説明する図である。

図37は、フォーマット・タイプ1におけるコンテンツチェック値ICV_iの生成処理方法を説明する図である。

図38は、フォーマット・タイプ2, 3における総チェック値、記録再生器固有チェック値の生成処理方法を説明する図である。

図39は、フォーマット・タイプ0, 1におけるコンテンツダウンロード処理の処理フローを示す図である。

図40は、フォーマット・タイプ2におけるコンテンツダウンロード処理の処理フローを示す図である。

図41は、フォーマット・タイプ3におけるコンテンツダウンロード処理の処理フローを示す図である。

図42は、フォーマット・タイプ0におけるコンテンツ再生処理の処理フローを示す図である。

図43は、フォーマット・タイプ1におけるコンテンツ再生処理の処理フローを示す図である。

図44は、フォーマット・タイプ2におけるコンテンツ再生処理の処理フローを示す図である。

図45は、フォーマット・タイプ3におけるコンテンツ再生処理の処理フローを示す図である。

図46は、コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図(その1)である。

図47は、コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成

、検証方法を説明する図（その２）である。

図４８は、コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図（その３）である。

図４９は、マスタ鍵を用いて各種の鍵を個別に生成する方法について説明する図である。

図５０は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例１）である。

図５１は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例２）である。

図５２は、マスタ鍵の使い分けにより、利用制限を実行する構成について説明する図である。

図５３は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例３）である。

図５４は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例４）である。

図５５は、マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例５）である。

図５６は、トリプルDESを適用した暗号鍵をシングルDESアルゴリズムを用いて格納する処理フローを示す図である。

図５７は、優先順位に基づくコンテンツ再生処理フロー（例１）を示す図である。

図５８は、優先順位に基づくコンテンツ再生処理フロー（例２）を示す図である。

図５９は、優先順位に基づくコンテンツ再生処理フロー（例３）を示す図である。

図６０は、コンテンツ再生処理における圧縮データの復号（伸長）処理を実行する構成について説明する図である。

図 6 1 は、コンテンツの構成例（例 1）を示す図である。

図 6 2 は、コンテンツの構成例 1 における再生処理フローを示す図である。

図 6 3 は、コンテンツの構成例（例 2）を示す図である。

図 6 4 は、コンテンツの構成例 2 における再生処理フローを示す図である。

図 6 5 は、コンテンツの構成例（例 3）を示す図である。

図 6 6 は、コンテンツの構成例 3 における再生処理フローを示す図である。

図 6 7 は、コンテンツの構成例（例 4）を示す図である。

図 6 8 は、コンテンツの構成例 4 における再生処理フローを示す図である。

図 6 9 は、セーブデータの生成、格納処理について説明する図である。

図 7 0 は、セーブデータの格納処理例(例 1)に関する処理フローを示す図である。

図 7 1 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（例 1）を示す図である。

図 7 2 は、セーブデータの再生処理例(例 1)に関する処理フローを示す図である。

図 7 3 は、セーブデータの格納処理例(例 2)に関する処理フローを示す図である。

図 7 4 は、セーブデータの再生処理例(例 2)に関する処理フローを示す図である。

図 7 5 は、セーブデータの格納処理例(例 3)に関する処理フローを示す図である。

図 7 6 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成（例 2）を示す図である。

図 7 7 は、セーブデータの再生処理例(例 3)に関する処理フローを示す図である。

図 7 8 は、セーブデータの格納処理例(例 4)に関する処理フローを示す図である。

図 7 9 は、セーブデータの再生処理例(例 4)に関する処理フローを示す図である。

図 8 0 は、セーブデータの格納処理例(例 5)に関する処理フローを示す図である。

図 8 1 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例 3)を示す図である。

図 8 2 は、セーブデータの再生処理例(例 5)に関する処理フローを示す図である。

図 8 3 は、セーブデータの格納処理例(例 6)に関する処理フローを示す図である。

図 8 4 は、セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例 4)を示す図である。

図 8 5 は、セーブデータの再生処理例(例 6)に関する処理フローを示す図である。

図 8 6 は、コンテンツ不正利用者排除(リボケーション)構成を説明する図である。

図 8 7 は、コンテンツ不正利用者排除(リボケーション)の処理フロー(例 1)を示す図である。

図 8 8 は、コンテンツ不正利用者排除(リボケーション)の処理フロー(例 2)を示す図である。

図 8 9 は、セキュリティチップの構成(例 1)を説明する図である。

図 9 0 は、セキュリティチップの製造方法における処理フローを示す図である。

図 9 1 は、セキュリティチップの構成(例 2)を説明する図である。

図 9 2 は、セキュリティチップ(例 2)におけるデータ書き込み処理における処理フローを示す図である。

図 9 3 は、セキュリティチップ(例 2)における書き込みデータチェック処理

における処理フローを示す図である。

発明を実施するための最良の形態

以下に本発明の実施の形態を説明する。説明の手順は、以下の項目に従って行なう。

- (1) データ処理装置構成
- (2) コンテンツデータフォーマット
- (3) データ処理装置において適用可能な暗号処理概要
- (4) 記録再生器の格納データ構成
- (5) 記録デバイスの格納データ構成
- (6) 記録再生器、記録デバイス間における相互認証処理
 - (6-1) 相互認証処理の概要
 - (6-2) 相互認証時の鍵ブロックの切り替え
- (7) 記録再生器から記録デバイスへのダウンロード処理
- (8) 記録デバイス格納情報の記録再生器での再生処理
- (9) 相互認証後の鍵交換処理
- (10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理
 - (11) コンテンツプロバイダにおけるチェック値 (ICV) 生成処理態様
 - (12) マスタ鍵に基づく暗号処理鍵生成構成
 - (13) 暗号処理における暗号強度の制御
 - (14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理
- (15) コンテンツ構成および再生(伸長)処理
- (16) セーブデータの生成および記録デバイスへの格納、再生処理
- (17) 不正機器の排除 (リボケーション) 構成
- (18) セキュアチップ構成および製造方法

(1) データ処理装置構成

図2に本発明のデータ処理装置の一実施例に係る全体構成ブロック図を示す。本発明のデータ処理装置は、記録再生器300と記録デバイス400とを主要構成要素とする。

記録再生器300は、例えばパーソナル・コンピュータ（PC：Personal Computer）、あるいはゲーム機器等によって構成される。記録再生器300は、図2に示すように、記録再生器300における暗号処理時の記録デバイス400との通信制御を含む統括的制御を実行する制御部301、暗号処理全般を司る記録再生器暗号処理部302、記録再生器に接続される記録デバイス400と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ303、DVDなどのメディア500から少なくともデータの読み出しを行う読み取り部304、外部とデータの送受信を行う通信部305を有する。

記録再生器300は、制御部301の制御により記録デバイス400に対するコンテンツデータのダウンロード、記録デバイス400からのコンテンツデータ再生を実行する。記録デバイス400は、記録再生器300に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、EEPROM、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきRAMなどによって構成される外部メモリ402を有する。

記録再生器300は、図2の左端に示す記憶媒体、DVD、CD、FD、HDDに格納されたコンテンツデータを入力可能なインタフェースとしての読み取り部304、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインタフェースとしての通信部305を有し、外部からコンテンツを入力する。

記録再生器300は、暗号処理部302を有し、読取部304または通信部305を介して外部から入力されるコンテンツデータを記録デバイス400にダウンロード処理する際、あるいはコンテンツデータを記録デバイス400から再生、実行する際の認証処理、暗号化处理、復号化处理、さらにデータの検証処理等

を実行する。暗号処理部 302 は、暗号処理部 302 全体を制御する制御部 306、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ 307、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部 308 から構成されている。

制御部 301 は、例えば、記録再生器 300 に記録デバイス 400 が装着された際に記録デバイスコントローラ 303 を介して記録デバイス 400 に初期化命令を送信したり、あるいは、記録再生器暗号処理部 302 の暗号／復号化部 308 と記録デバイス暗号処理部 401 の暗号／復号化部 406 の間で行われる相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。これらの各処理については、後段で詳細に説明する。

暗号処理部 302 は、前述のように認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、暗号処理制御部 306、内部メモリ 307、暗号／復号化部 308 を有する。

暗号処理制御部 306 は、記録再生器 300 において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、記録再生器 300 と記録デバイス 400 との間で実行される認証処理の完了時における認証完了フラグの設定、記録再生器暗号処理部 302 の暗号／復号化部 308 において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

内部メモリ 307 は、後段で詳細に説明するが、記録再生器 300 において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等を格納する。

暗号／復号化部 308 は、内部メモリ 307 に格納された鍵データ等を使用して、外部から入力されるコンテンツデータを記録デバイス 400 にダウンロード処理する際、あるいは記録デバイス 400 に格納されたコンテンツデータを記録

デバイス400から再生、実行する際の認証処理、暗号化処理、復号化処理、さらに所定のチェック値や電子署名の生成・検証、データの検証、乱数の発生などの処理を実行する。

ここで、記録再生器暗号処理部302の内部メモリ307は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部302は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。この構成については、後段で詳細に説明する。

記録再生器300は、これらの暗号処理機能の他に、中央演算処理装置（メインCPU：Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108、AV処理部109、入力インタフェース110、PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112を備えている。

中央演算処理装置（メインCPU：Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108は、記録再生器300本体の制御系として機能する構成部であり、主として記録再生器暗号処理部302で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインCPU：Central Processing Unit）106は、制御部301の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをAV処理部109へ出力する等、コンテンツの再生、実行に関する制御を行なう。

RAM107は、CPU106における各種処理用の主記憶メモリとして使用

され、メインCPU106による処理のための作業領域として使用される。ROM108は、メインCPU106で起動されるOS等を立ち上げるための基本プログラム等が格納される。

AV処理部109は、具体的には、例えばMPEG2デコーダ、ATRACデコーダ、MP3デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

入力インタフェース110は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインCPU106に出力する。メインCPU106は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。

PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112は、メモ리카ード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インタフェースとして使用される。

また、メインCPU106は、例えば実行中のゲーム等に関する設定データ等をセーブデータとして記録デバイス400に記憶する際の制御も行なう。この処理の際には、記憶データを制御部301に転送し、制御部301は必要に応じて暗号処理部302にセーブデータに関する暗号処理を実行させ、暗号化データを記録デバイス400に格納する。これらの暗号処理については、後段で詳細に説明する。

記録デバイス400は、前述したように好ましくは記録再生器300に対して着脱可能な記憶媒体であり、例えばメモ리카ードによって構成される。記録デバイス400は暗号処理部401、外部メモリ402を有する。

記録デバイス暗号処理部401は、記録再生器300からのコンテンツデータのダウンロード、または記録デバイス400から記録再生器300へのコンテンツデータの再生処理時等における記録再生器300と記録デバイス400間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処

理部であり、記録再生器 300 の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。これらの詳細は図 3 に示す。外部メモリ 402 は、前述したように、例えば EEPROM 等のフラッシュメモリからなる不揮発メモリ、ハードディスク、電池つき RAM などによって構成され、暗号化されたコンテンツデータ等を格納する。

図 3 は、本発明のデータ処理装置がデータ供給を受けるコンテンツ提供手段であるメディア 500、通信手段 600 から入力されるデータ構成の概略を示すとともに、これらコンテンツ提供手段 500、600 からコンテンツを入力する記録再生器 300 と、記録デバイス 400 における暗号処理に関する構成を中心として、その構成を示した図である。

メディア 500 は、例えば光ディスクメディア、磁気ディスクメディア、磁気テープメディア、半導体メディア等である。通信手段 600 は、インターネット通信、ケーブル通信、衛星通信等の、データ通信可能な手段である。

図 3 において、記録再生器 300 は、コンテンツ提供手段であるメディア 500、通信手段 600 から入力されるデータ、すなわち図 3 に示すような所定のフォーマットに従ったコンテンツを検証し、検証後にコンテンツを記録デバイス 400 に保存する。

図 3 のメディア 500、通信手段 600 部分に示すようにコンテンツデータは以下のような構成部を有する。

識別情報：コンテンツデータの識別子としての識別情報。

取扱方針：コンテンツデータの構成情報、例えばコンテンツデータを構成するヘッダー部サイズ、コンテンツ部サイズ、フォーマットのバージョン、コンテンツがプログラムかデータか等を示すコンテンツタイプ、さらにコンテンツがダウンロードした機器だけでしか利用できないのか他の機器でも利用できるのか等の利用制限情報等を含む取扱方針。

ブロック情報：コンテンツブロックの数、ブロックサイズ、暗号化の有無を示す暗号化フラグ等から構成されるブロック情報。

鍵データ：上述のブロック情報を暗号化する暗号化鍵、あるいはコンテンツブロックを暗号化するコンテンツ鍵等からなる鍵データ。

コンテンツブロック：実際の再生対象となるプログラムデータ、音楽、画像データ等からなるコンテンツブロック。

を有する。なお、コンテンツデータ詳細については、後段で図 4 以下を用いてさらに詳細に説明する。

コンテンツデータは、コンテンツ鍵（ここでは、これをコンテンツ鍵（Content Key（以下、Kconとする））と呼ぶ）によって暗号化されて、メディア 500、通信手段 600 から記録再生器 300 に提供される。コンテンツは、記録再生器 300 を介して記録デバイス 400 の外部メモリに格納することができる。

例えば、記録デバイス 400 は、記録デバイス内の内部メモリ 405 に格納された記録デバイス固有の鍵（ここでは、これを保存鍵（Storage Key（以下、Kstrとする））と呼ぶ）を用いて、コンテンツデータに含まれるコンテンツ、及びコンテンツデータのヘッダ情報として含まれるブロック情報、各種鍵情報、例えばコンテンツ鍵 Kcon などを暗号化して外部メモリ 402 に記憶する。コンテンツデータの記録再生器 300 から記録デバイス 400 へのダウンロード処理、あるいは記録再生器 300 による記録デバイス 400 内に格納されたコンテンツデータの再生処理においては、機器間の相互認証処理、コンテンツデータの暗号化、復号化処理等、所定の手続きが必要となる。これらの処理については、後段で詳細に説明する。

記録デバイス 400 は、図 3 に示すように暗号処理部 401、外部メモリ 402 を有し、暗号処理部 401 は、制御部 403、通信部 404、内部メモリ 405、暗号／復号化部 406、外部メモリ制御部 407 を有する。

記録デバイス 400 は、暗号処理全般を司り、外部メモリ 402 を制御するとともに、記録再生器 300 からのコマンドを解釈し、処理を実行する記録デバイス暗号処理部 401 と、コンテンツなどを保持する外部メモリ 402 からなる。

記録デバイス暗号処理部 401 は、記録デバイス暗号処理部 401 全体を制御する制御部 403、記録再生器 300 とデータの送受信を行う通信部 404、暗号処理用の鍵データなどの情報を保持し、外部から容易に読み出せないように処理が施された内部メモリ 405、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部 406、外部メモリ 402 のデータを読み書きする外部メモリ制御部 407 を有する。

制御部 403 は、記録デバイス 400 において実行される認証処理、暗号化／復号化処理等の暗号処理全般に係る制御を実行する制御部であり、例えば、記録再生器 300 と記録デバイス 400 との間で実行される認証処理の完了時における認証完了フラグの設定、暗号処理部 401 の暗号／復号化部 406 において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

内部メモリ 405 は、後段で詳細に説明するが、複数のブロックを持つメモリによって構成されており、記録デバイス 400 において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等の組を複数格納した構成となっている。

記録デバイス暗号処理部 401 の内部メモリ 405 は、先に説明した記録再生器暗号処理部 302 の内部メモリ 307 と同様、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録デバイス 400 の暗号処理部 401 は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされる。なお、記録再生器暗号処理部 302 は、鍵などの秘密の情報を容易に外部に漏らさないように構成されたソフトウェアであってもよい。

暗号／復号化部 406 は、記録再生器 300 からのコンテンツデータのダウン

ロード処理、記録デバイス 400 の外部メモリ 402 に格納されたコンテンツデータの再生処理、あるいは、記録再生器 300 と記録デバイス 400 間の相互認証処理の際、内部メモリ 405 に格納された鍵データ等を使用して、データの検証処理、暗号化処理、復号化処理、所定のチェック値や電子署名の生成・検証、乱数の発生などの処理等を実行する。

通信部 404 は、記録再生器 300 の記録デバイスコントローラ 303 に接続され、記録再生器 300 の制御部 301、あるいは、記録デバイス 403 の制御部 403 の制御に従って、コンテンツデータのダウンロード処理、再生処理、あるいは、相互認証処理の際の記録再生器 300 と記録デバイス 400 間の転送データの通信を行なう。

(2) コンテンツデータフォーマット

次に、図 4 乃至図 6 を用いて、本発明のシステムにおけるメディア 500 に格納され、またはデータ通信手段 600 上を流通するデータのデータフォーマットについて説明する。

図 4 に示す構成がコンテンツデータ全体のフォーマットを示す図であり、図 5 に示す構成がコンテンツデータのヘッダ部の一部を構成する「取扱方針」の詳細を示す図であり、図 6 に示す構成がコンテンツデータのヘッダ部の一部を構成する「ブロック情報」の詳細を示す図である。

なお、ここでは、本発明のシステムにおいて適用されるデータフォーマットの代表的な一例について説明するが、本発明のシステムでは、例えばゲームプログラムに対応したフォーマット、音楽データ等のリアルタイム処理に適したフォーマット等、異なる複数のデータフォーマットが利用可能であり、これらのフォーマットの態様については、後段「(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」において、さらに詳しく述べる。

図 4 に示すデータフォーマットにおいて、グレーで示す部分は暗号化されたデータであり、二重枠の部分は改竄チェックデータ、その他の白い部分は暗号化さ

れていない平文のデータである。暗号化部の暗号化鍵は、それぞれの枠の左に示す鍵である。図4に示す例においては、コンテンツ部の各ブロック（コンテンツブロックデータ）に暗号化されたものと暗号化されていないものとが混在している。これらの形態は、コンテンツデータに応じて異なるものであり、データに含まれるすべてのコンテンツブロックデータが暗号化されている構成であってもよい。

図4に示すように、データフォーマットは、ヘッダー部とコンテンツ部に分かれており、ヘッダー部は、識別情報（Content ID）、取扱方針（Usage Policy）、チェック値A（Integrity Check Value A（以下、ICVaとする））、ブロック情報鍵（Block Information Table Key（以下、Kbitとする））、コンテンツ鍵Kcon、ブロック情報（Block Information Table（以下、BITとする））、チェック値B（ICVb）、総チェック値（ICVt）により構成されており、コンテンツ部は、複数のコンテンツブロック（例えば暗号化されたコンテンツと、暗号化されていないコンテンツ）から構成されている。

ここで、識別情報は、コンテンツを識別するための個別の識別子（Content ID）を示している。取扱方針は、図5にその詳細を示すように、ヘッダー部分のサイズを示すヘッダーサイズ（Header Length）、コンテンツ部分のサイズを示すコンテンツサイズ（Content Length）、フォーマットのバージョン情報を示すフォーマットバージョン（Format Version）、フォーマットの種類を示すフォーマットタイプ（Format Type）、コンテンツ部に保存されているコンテンツがプログラムなのか、データなのか等コンテンツの種類を示すコンテンツタイプ（Content Type）、コンテンツタイプがプログラムである場合の起動優先順位を示す起動優先順位情報（Operation Priority）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした

機器だけでしか利用できないのか、他の同様な機器でも利用できるのかを示す利用制限情報 (Localization Field)、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に複製できるのか否かを示す複製制限情報 (Copy Permission)、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に移動できるのか否かを示す移動制限情報 (Move Permission)、コンテンツ部内のコンテンツブロックを暗号するのに使用したアルゴリズムを示す暗号アルゴリズム (Encryption Algorithm)、コンテンツ部内のコンテンツを暗号化するのに使用したアルゴリズムの使用方法を示す暗号化モード (Encryption Mode)、チェック値の生成方法を示す検証方法 (Integrity Check Method) から構成されている。

なお、上述した取扱方針に記録するデータ項目は、1つの例であり、対応するコンテンツデータの態様に応じて様々な取扱方針情報を記録することが可能である。例えば後段の「(17) 不正機器の排除 (リボケーション) 構成」で詳しく述べるが、不正な記録再生器の識別子をデータとして記録して、利用開始時の照合によって不正機器によるコンテンツ利用を排除するように構成することも可能である。

チェック値A, ICVaは、識別情報、取扱方針の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。データブロック情報鍵Kbitは、ブロック情報を暗号化するのに用いられ、コンテンツ鍵Kconは、コンテンツブロックを暗号化するのに用いられる。なお、ブロック情報鍵Kbit及びコンテンツ鍵Kconは、メディア500上および通信手段600上では後述する配送鍵 (Distribution Key (以下、Kdisとする)) で暗号化されている。

ブロック情報の詳細を図6に示す。なお、図6のブロック情報は、図4から理

解されるようにすべてブロック情報鍵 K_{bit} によって暗号化されているデータである。ブロック情報は、図6に示すように、コンテンツブロックの数を示すコンテンツブロック数 ($Block\ Number$) と N 個のコンテンツブロック情報から構成されている。コンテンツブロック情報は、ブロックサイズ ($Block\ Length$)、暗号化されているか否かを示す暗号化フラグ ($Encryption\ Flag$)、チェック値を計算する必要があるか否かを示す検証対象フラグ ($ICV\ Flag$)、コンテンツチェック値 (ICV_i) から構成されている。

コンテンツチェック値は、各コンテンツブロックの改竄を検証するために用いられるチェック値である。コンテンツチェック値の生成手法の具体例については、後段の「(10) 複数のデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理」の欄で説明する。なお、ブロック情報を暗号化しているブロック情報鍵 K_{bit} は、さらに、配送鍵 K_{dis} によって暗号化されている。

図4のデータフォーマットの説明を続ける。チェック値 B 、 ICV_b は、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} 、ブロック情報の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。総チェック値 ICV_t は、 ICV_a 、 ICV_b 、各コンテンツブロックのチェック値 ICV_i (設定されている場合)、これらの部分チェック値、あるいはそのチェック対象となるデータ全ての改竄を検証するためのチェック値である。

なお、図6においては、ブロックサイズ、暗号化フラグ、検証対象フラグを自由に設定できるようにしているが、ある程度ルールを決めた構成としてもよい。例えば、暗号文領域と平文領域を固定サイズ繰り返しにしたり、全コンテンツデータを暗号化したりし、ブロック情報 BIT を圧縮してもよい。また、コンテンツ鍵 K_{con} をコンテンツブロック毎に異なるようにするため、コンテンツ鍵 K_{con} をヘッダー部分ではなく、コンテンツブロックに含ませるようにしてもよ

い。コンテンツデータフォーマットの例については、「(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」の項目において、さらに詳細に説明する。

(3) 本発明のデータ処理装置において適用可能な暗号処理概要

次に、本発明のデータ処理装置において適用され得る各種暗号処理の態様について説明する。なお、本項目「(3) 本発明のデータ処理装置において適用可能な暗号処理の概要」に示す暗号処理に関する説明は、後段で具体的に説明する本発明のデータ処理装置における各種処理、例えば a. 記録再生器と記録デバイス間での認証処理。 b. コンテンツの記録デバイスに対するダウンロード処理。 c. 記録デバイスに格納したコンテンツの再生処理等の処理において実行される処理の基礎となる暗号処理の態様について、その概要を説明するものである。記録再生器 300 と記録デバイス 400 における具体的処理については、本明細書の項目 (4) 以下において、各処理毎に詳細に説明する。

以下、データ処理装置において適用可能な暗号処理の概要について、

- (3-1) 共通鍵暗号方式によるメッセージ認証
- (3-2) 公開鍵暗号方式による電子署名
- (3-3) 公開鍵暗号方式による電子署名の検証
- (3-4) 共通鍵暗号方式による相互認証
- (3-5) 公開鍵証明書
- (3-6) 公開鍵暗号方式による相互認証
- (3-7) 楕円曲線暗号を用いた暗号化処理
- (3-8) 楕円曲線暗号を用いた復号化処理
- (3-9) 乱数生成処理

の順に説明する。

(3-1) 共通鍵暗号方式によるメッセージ認証

まず、共通鍵暗号方式を用いた改竄検出データの生成処理について説明する。改竄検出データは、改竄の検出を行ないたいデータに付け、改竄のチェックおよ

び作成者認証をするためのデータである。

例えば、図4で説明したデータ構造中の二重枠部分の各チェック値A、B、総チェック値、および図6に示すブロック情報中の各ブロックに格納されたコンテンツチェック値等が、この改竄検出データとして生成される。

ここでは、電子署名データの生成処理方法の例の1つとして共通鍵暗号方式におけるDESを用いた例を説明する。なお、本発明においては、DES以外にも、同様の共通鍵暗号方式における処理として例えばFEAL (Fast Encryption Algorithm: NTT)、AES (Advanced Encryption Standard: 米国次期標準暗号) 等を用いることも可能である。

一般的なDESを用いた電子署名の生成方法を図7を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを8バイト単位に分割する(以下、分割されたメッセージをM1、M2、・・・、MNとする)。そして、初期値 (Initial Value (以下、IVとする)) とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENが電子署名になる。この値は一般にはメッセージ認証符号 (MAC (Message Authentication Code)) と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをCBC (Cipher Block Chaining) モードと呼ぶ。

なお、図7のような生成例において出力されるMAC値が、図4で示すデータ構造中の二重枠部分の各チェック値A、B、総チェック値、および図6に示すブロック情報中の各ブロックに格納されたコンテンツチェック値ICV1～ICVNとして使用可能である。このMAC値の検証時には、検証者が生成時と同様の

方法でMAC値を生成し、同一の値が得られた場合、検証成功とする。

なお、図7に示す例では初期値IVを、初めの8バイトメッセージM1に排他的論理和したが、初期値IV=0として、初期値を排他的論理和しない構成とすることも可能である。

図7に示すMAC値生成方法に対して、さらにセキュリティを向上させたMAC値生成方法を示す処理構成図を図8に示す。図8は、図7のシングルDESに代えてトリプルDES (Triple DES) を用いてMAC値の生成を実行する例を示したものである。

図8に示す各トリプルDES (Triple DES) 構成部の詳細構成例を図9に示す。図9(a)、(b)に示すようにトリプルDES (Triple DES) としての構成には2つの異なる態様がある。図9(a)は、2つの暗号鍵を用いた例を示すものであり、鍵1による暗号化処理、鍵2による復号化処理、さらに鍵1による暗号化処理の順に処理を行う。鍵は、K1、K2、K1の順に2種類用いる。図9(b)は3つの暗号鍵を用いた例を示すものであり、鍵1による暗号化処理、鍵2による暗号化処理、さらに鍵3による暗号化処理の順に処理を行い3回とも暗号化処理を行う。鍵は、K1、K2、K3の順に3種類の鍵を用いる。このように複数の処理を連続させる構成とすることで、シングルDESに比較してセキュリティ強度を向上させている。しかしながら、このトリプルDES (Triple DES) 構成は、処理時間がシングルDESのおよそ3倍かかるという欠点を有する。

図8および図9で説明したトリプルDES構成を改良したMAC値生成構成例を図10に示す。図10においては、署名対象となるメッセージ列の初めから途中までの各メッセージに対する暗号化処理は全てシングルDESによる処理とし、最後のメッセージに対する暗号化処理のみを図9(a)に示すトリプルDES (Triple DES) 構成としたものである。

図10に示すこのような構成とすることで、メッセージのMAC値の生成処理時間は、シングルDESによるMAC値生成処理に要する時間とほぼ同程度に短

縮され、かつセキュリティはシングルDESによるMAC値よりも高めることが可能となる。なお、最終メッセージに対するトリプルDES構成は、図9(b)の構成とすることも可能である。

(3-2) 公開鍵暗号方式による電子署名

以上は、暗号化方式として共通鍵暗号化方式を適用した場合の電子署名データの生成方法であるが、次に、暗号化方式として公開鍵暗号方式を用いた電子署名の生成方法を図11を用いて説明する。図11に示す処理は、ECDSA (Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3)を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号 (Elliptic Curve Cryptography (以下、ECCと呼ぶ))を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばRSA暗号 (Rivest, Shamir, Adleman) など (ANSI X9.31)を用いることも可能である。

図11の各ステップについて説明する。ステップS1において、 p を標数、 a 、 b を楕円曲線の係数 (楕円曲線: $y^2 = x^3 + ax + b$)、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵 ($0 < K_s < r$)とする。ステップS2において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値 (出力) から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、図7他で説明したと同様のDES-CBCが用いられる場合もある。この場合は、最終出

力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

続けて、ステップS3で、乱数 u （ $0 < u < r$ ）を生成し、ステップS4でベースポイントを u 倍した座標 $V(X_v, Y_v)$ を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

$P = (X_a, Y_a)$, $Q = (X_b, Y_b)$, $R = (X_c, Y_c) = P + Q$ とすると

、
 $P \neq Q$ のとき、（加算）、

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P = Q$ の時（2倍算）、

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a) \quad \dots\dots (1)$$

これらを用いて点 G の u 倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。 G 、 $2 \times G$ 、 $4 \times G \dots$ を計算し、 u を2進数展開して1が立っているところに対応する $2^i \times G$ （ G を i 回2倍算した値）を加算する（ i は u のLSBから数えた時のビット位置））。

ステップS5で、 $c = X_v \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cK_s) / u] \bmod r$ を計算し、ステップS8で d が0であるかどうか判定し、 d が0でなければ、ステップS9で c および d を電子署名データとして出力する。仮に、 r を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

ステップS6において、 c が0であった場合、ステップS3に戻って新たな乱

数を生成し直す。同様に、ステップS 8でdが0であった場合も、ステップS 3に戻って乱数を生成し直す。

(3-3) 公開鍵暗号方式による電子署名の検証

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図12を用いて説明する。ステップS 11で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、Gおよび $K_s \times G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS 12で電子署名データcおよびdが $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップS 13で、メッセージMのハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。次に、ステップS 14で $h = 1/d \bmod r$ を計算し、ステップS 15で $h_1 = fh \bmod r$ 、 $h_2 = ch \bmod r$ を計算する。

ステップS 16において、既に計算した h_1 および h_2 を用い、点 $P = (X_p, Y_p) = h_1 \times G + h_2 \cdot K_s \times G$ を計算する。電子署名検証者は、公開鍵Gおよび $K_s \times G$ を知っているので、図11のステップS 4と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップS 17で点Pが無限遠点かどうか判定し、無限遠点でなければステップS 18に進む（実際には、無限遠点の判定はステップS 16でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、 λ が計算できず、 $P + Q$ が無限遠点であることが判明している）。ステップS 18で $X_p \bmod r$ を計算し、電子署名データcと比較する。最後に、この値が一致していた場合、ステップS 19に進み、電子署名が正しいと判定する。

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

ステップS 12において、電子署名データcまたはdが、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップS 20に進む。また、ステップS 17において、点Pが無限遠点であった場合もステップS 20に進む。さらにまた、ステ

ップS18において、 $X_p \bmod r$ の値が、電子署名データcと一致していなかった場合にもステップS20に進む。

ステップS20において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

(3-4) 共通鍵暗号方式による相互認証

次に、共通鍵暗号方式を用いた相互認証方法を、図13を用いて説明する。図13において、共通鍵暗号方式としてDESを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図13において、まず、Bが64ビットの乱数Rbを生成し、Rbおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra、Rb、ID(b)の順に、DESのCBCモードで鍵Kabを用いてデータを暗号化し、Bに返送する。図7に示すDESのCBCモード処理構成によれば、RaがM1、RbがM2、ID(b)がM3に相当し、初期値：IV=0としたときの出力E1、E2、E3が暗号文となる。

これを受信したBは、受信データを鍵Kabで復号化する。受信データの復号化方法は、まず、暗号文E1を鍵Kabで復号化し、乱数Raを得る。次に、暗号文E2を鍵Kabで復号化し、その結果とE1を排他的論理和し、Rbを得る。最後に、暗号文E3を鍵Kabで復号化し、その結果とE2を排他的論理和し、ID(b)を得る。こうして得られたRa、Rb、ID(b)の内、RbおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

次にBは、認証後に使用するセッション鍵 (Session Key (以下、Ksesとする)) を生成する (生成方法は、乱数を用いる)。そして、Rb、Ra、Ksesの順に、DESのCBCモードで鍵Kabを用いて暗号化し、Aに返送する。

これを受信したAは、受信データを鍵Kabで復号化する。受信データの復号

化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた R_b 、 R_a 、 K_{ses} の内、 R_b および R_a が、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッション鍵 K_{ses} は、認証後の秘密通信のための共通鍵として利用される。

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

(3-5) 公開鍵証明書

次に、公開鍵証明書について図14を用いて説明する。公開鍵証明書は、公開鍵暗号方式における認証局(CA: Certificate Authority)が発行する証明書であり、ユーザが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

図14に示す公開鍵証明書は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前(ユーザID)、証明書利用者の公開鍵並びに電子署名を含む。

電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。この電子署名の生成には、例えば図11で説明した処理フローが適用される。

認証局は、図14に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布(これをリボケーション: Revocationと呼ぶ)を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図12で説明したのでその詳細は省略する。

(3-6) 公開鍵暗号方式による相互認証

次に、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数 R_b を生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数 R_a および標数 p より小さい乱数 A_k を生成する。そして、ベースポイント G を A_k 倍した点 $A_v = A_k \times G$ を求め、 R_a 、 R_b 、 A_v （X座標とY座標）に対する電子署名 $A.Sig$ を生成し、Aの公開鍵証明書とともにBに返送する。ここで、 R_a および R_b はそれぞれ64ビット、 A_v のX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。電子署名の生成方法は図11で説明したので、その詳細は省略する。また、公開鍵証明書も図14で説明したので、その詳細は省略する。

Aの公開鍵証明書、 R_a 、 R_b 、 A_v 、電子署名 $A.Sig$ を受信したBは、Aが送信してきた R_b が、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。公開鍵証明書の検証については、図14を用いて説明したので、その詳細は省略する。そして、取り出したAの公開鍵を用い電子署名 $A.Sig$ を検証する。電子署名の検証方法は図12で説明したので、その詳細は省略する。電子署名の検証に成功した後、BはAを正当なものとして認証する。

次に、Bは、標数 p より小さい乱数 B_k を生成する。そして、ベースポイント G を B_k 倍した点 $B_v = B_k \times G$ を求め、 R_b 、 R_a 、 B_v (X座標とY座標) に対する電子署名 $B.Sig$ を生成し、Bの公開鍵証明書とともにAに返送する。

Bの公開鍵証明書、 R_b 、 R_a 、 A_v 、電子署名 $B.Sig$ を受信したAは、Bが送信してきた R_a が、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名 $B.Sig$ を検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

両者が認証に成功した場合には、Bは $B_k \times A_v$ (B_k は乱数だが、 A_v は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要) を計算し、Aは $A_k \times B_v$ を計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する (共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合)。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

(3-7) 楕円曲線暗号を用いた暗号化処理

次に、楕円曲線暗号を用いた暗号化について、図16を用いて説明する。ステップS21において、 M_x 、 M_y をメッセージ、 p を標数、 a 、 b を楕円曲線の係数 (楕円曲線: $y^2 = x^3 + ax + b$)、 G を楕円曲線上のベースポイント、 r を G の位数、 G および $K_s \times G$ を公開鍵 ($0 < K_s < r$) とする。ステップS22で乱数 u を $0 < u < r$ になるように生成し、ステップS23で公開鍵 $K_s \times G$ を u 倍した座標 V を計算する。なお、楕円曲線上のスカラー倍は図11のステップS4で説明したので、詳細は省略する。ステップS24で、 V のX座標を M_x 倍

して p で剰余を求め X_0 とし、ステップ S 2 5 で V の Y 座標を M_y 倍して p で剰余を求め Y_0 とする。なお、メッセージの長さが p のビット数より少ない場合、 M_y は乱数を使い、復号化部では M_y を破棄するようにする。ステップ S 2 6 において、 $u \times G$ を計算し、ステップ S 2 7 で暗号文 $u \times G$ 、 (X_0, Y_0) を得る。

(3-8) 楕円曲線暗号を用いた復号化处理

次に、楕円曲線暗号を用いた復号化について、図 1 7 を用いて説明する。ステップ S 3 1 において、 $u \times G$ 、 (X_0, Y_0) を暗号文データ、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵（ $0 < K_s < r$ ）とする。ステップ S 3 2 において、暗号データ $u \times G$ を秘密鍵 K_s 倍し、座標 $V (X_v, Y_v)$ を求める。ステップ S 3 3 では、暗号データの内、 (X_0, Y_0) の X 座標を取り出し、 $X_1 = X_0 / X_v \bmod p$ を計算し、ステップ S 3 4 においては、 Y 座標を取り出し、 $Y_1 = Y_0 / Y_v \bmod p$ を計算する。そして、ステップ S 3 5 で X_1 を M_x とし、 Y_1 を M_y としてメッセージを取り出す。この時、 M_y をメッセージにしていなかった場合、 Y_1 は破棄する。

このように、秘密鍵を K_s 、公開鍵を G 、 $K_s \times G$ とすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができる。

また、公開鍵暗号の他の例としては RSA 暗号が知られているが、詳しい説明は省略する（PKCS # 1 Version 2 に詳細が記述されている）。

(3-9) 乱数生成処理

次に、乱数の生成方法について説明する。乱数の生成方法としては、熱雑音を増幅し、その A/D 出力から生成する真性乱数生成法や、M 系列等の線形回路を複数組み合わせ生成する疑似乱数生成法等が知られている。また、DES 等の共通鍵暗号を用いて生成する方法も知られている。本例では、DES を用いた疑似乱数生成方法について説明する（ANSI X 9. 1 7 ベース）。

まず、時間等のデータから得られた 6 4 ビット（これ以下のビット数の場合、

上位ビットを0とする)の値をD、Triple-DESに使われる鍵情報をK_r、乱数発生用の種(Seed)をSとする。このとき、乱数Rは以下のように計算される。

$$I = \text{Triple-DES}(K_r, D) \cdots \cdots (2-1)$$

$$R = \text{Triple-DES}(K_r, S \wedge I) \cdots \cdots (2-2)$$

$$S = \text{Triple-DES}(K_r, R \wedge I) \cdots \cdots (2-3) \quad \cdots \cdots (2)$$

ここで、Triple-DES()は、第1引数を暗号鍵情報として、第2引数の値をTriple-DESで暗号化する関数とし、演算 \wedge は64ビット単位の排他的論理和、最終的にでてきた値Sは、新規のSeed(種)として更新されていくものとする。

以下、連続して乱数を生成する場合には、(2-2)式、(2-3)式を繰り返すものとする。

以上、本発明のデータ処理装置において適用可能な暗号処理に関する各種処理態様について説明した。次に、本発明のデータ処理装置において実行される具体的な処理について、詳細に説明する。

(4) 記録再生器の格納データ構成

図18は、図3で示す記録再生器300での記録再生器暗号処理部302に構成された内部メモリ307のデータ保持内容を説明する図である。

図18に示すように、内部メモリ307には、以下の鍵、データが格納されている。

MKake : 記録再生器300と記録デバイス400(図3参照)との間で実行される相互認証処理に必要な認証鍵(Authentication and Key Exchange Key(以下、Kakeとする))を生成するための記録デバイス認証鍵用マスター鍵。

IVake : 記録デバイス認証鍵用初期値。

MKdis : 配送鍵 **Kdis** を生成するための配送鍵用マスター鍵。

IVdis : 配送鍵生成用初期値。

Kicva : チェック値 **ICVa** を生成するための鍵であるチェック値 A 生成鍵。

Kicvb : チェック値 **ICVb** を生成するための鍵であるチェック値 B 生成鍵。

Kicvc : 各コンテンツブロックのチェック値 **ICVi** ($i = 1 \sim N$) を生成するための鍵であるコンテンツチェック値生成鍵。

Kicvt : 総チェック値 **ICVt** を生成するための鍵である総チェック値生成鍵。

Ksys : 配信システムに共通の署名または **ICV** をつけるために使用するシステム署名鍵。

Kdev : 記録再生器毎に異なり、記録再生器が署名または **ICV** をつけるために使用する記録再生器固有の記録再生器署名鍵。

IVmem : 初期値、相互認証処理等の際の暗号処理に用いられる初期値。記録デバイスと共通。

これらの鍵、データが記録再生器暗号処理部 302 に構成された内部メモリ 307 に格納されている。

(5) 記録デバイスの格納データ構成

図 19 は、記録デバイス上でのデータ保持状況を示す図である。図 19 において、内部メモリ 405 は、複数のブロック（本例では N ブロック）に分割されており、それぞれのブロック中に、以下の鍵、データが格納されている。

IDmem : 記録デバイス識別情報、記録デバイス固有の識別情報。

Kake : 認証鍵、記録再生器 300 との相互認証時に用いる認証鍵。

IVmem : 初期値、相互認証処理等の際の暗号処理に用いられる初期値。

Kstr : 保存鍵、ブロック情報鍵他のコンテンツデータの暗号鍵。

Kr : 乱数生成鍵、

S：種

これらのデータを個別のブロックに各々保持している。外部メモリ402は複数（本例ではM個）のコンテンツデータを保持しており、それぞれ図4で説明したデータを、例えば図26、または図27のように保持している。図26、図27の構成の差異については後段で説明する。

（6）記録再生器、記録デバイス間における相互認証処理

（6－1）相互認証処理の概要

図20は、記録再生器300と記録デバイス400との認証手順を示す流れ図である。ステップS41において、利用者が記録デバイス400を記録再生器300に挿入する。ただし非接触で通信できる記録デバイスを使用する場合には、挿入する必要はない。

記録再生器300に記録デバイス400をセットすると、図3に示す記録再生器300内の記録デバイス検知手段（図示せず）が、制御部301に記録デバイス400の装着を通知する。次に、ステップS42において、記録再生器300の制御部301は、記録デバイスコントローラ303を介して記録デバイス400に初期化命令を送信する。これを受信した記録デバイス400は、記録デバイス暗号処理部401の制御部403において、通信部404を介して命令を受信し、認証完了フラグがセットされていればクリアする。すなわち未認証状態に設定する。

次に、ステップS43において、記録再生器300の制御部301は、記録再生器暗号処理部302に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器300に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス400との認証処理、およびデータ送受信が可能となる。

初期化命令を受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の制御部306において、記録デバイス挿入口番号に対応する認証完了フラグがセットされていればクリアする。すなわち未認証状態

に設定する。

次に、ステップS 4 4において、記録再生器3 0 0の制御部3 0 1は、記録デバイス4 0 0の記録デバイス暗号処理部4 0 1が使う鍵ブロック番号を指定する。なお、鍵ブロック番号の詳細に関しては後述する。ステップS 4 5において、記録再生器3 0 0の制御部3 0 1は、記録デバイス4 0 0の内部メモリ4 0 5の指定された鍵ブロックに格納された記録デバイス識別情報IDmemを読み出す。ステップS 4 6において、記録再生器3 0 0の制御部3 0 1は、記録再生器暗号処理部3 0 2に記録デバイス識別情報IDmemを送信し、記録デバイス識別情報IDmemに基づく認証鍵Kakeを生成させる。認証鍵Kakeの生成方法としては、例えば次のように生成する。

$$Kake = DES (MKake, IDmem \wedge IVake) \quad \dots\dots (3)$$

ここで、MKakeは、記録再生器3 0 0と記録デバイス4 0 0（図3参照）との間で実行される相互認証処理に必要な認証鍵Kakeを生成するための記録デバイス認証鍵用マスター鍵であり、これは、前述したように記録再生器3 0 0の内部メモリ3 0 7に格納されている鍵である。またIDmemは、記録デバイス4 0 0に固有の記録デバイス識別情報である。さらにIVakeは、記録デバイス認証鍵用初期値である。また、上記式において、DES（）は、第1引数を暗号鍵として、第2引数の値をDESで暗号化する関数であり、演算 \wedge は64ビット単位の排他的論理和を示す。

例えば図7、図8に示すDES構成を適用する場合には、図7、8に示されるメッセージMを記録デバイス識別情報：IDmemとし、鍵K1をデバイス認証鍵用マスター鍵：MKakeとし、初期値IVを：IVakeとして得られる出力が認証鍵Kakeとなる。

次に、ステップS 4 7で相互認証およびセッション鍵Ksesの生成処理を行う。相互認証は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8と記録デ

バイス暗号処理部 401 の暗号／復号化部 406 の間で行われ、その仲介を記録再生器 300 の制御部 301 が行っている。

相互認証処理は、例えば前述の図 13 で説明した処理にしたがって実行することができる。図 13 に示す構成において、A、B がそれぞれ記録再生器 300 と記録デバイス 400 に対応する。まず、記録再生器 300 の記録再生器暗号処理部 302 が乱数 R_b を生成し、乱数 R_b および自己の ID である記録再生器識別情報 ID_{dev} を記録デバイス 400 の記録デバイス暗号処理部 401 に送信する。なお、記録再生器識別情報 ID_{dev} は、記録再生器 300 内に構成された記憶部に記憶された再生器固有の識別子である。記録再生器暗号処理部 302 の内部メモリ中に記録再生器識別情報 ID_{dev} を記録する構成としてもよい。

乱数 R_b および記録再生器識別情報 ID_{dev} を受信した記録デバイス 400 の記録デバイス暗号処理部 401 は、新たに 64 ビットの乱数 R_a を生成し、 R_a 、 R_b 、と記録再生器識別情報 ID_{dev} の順に、DES の CBC モードで認証鍵 K_{ake} を用いてデータを暗号化し、記録再生器 300 の記録再生器暗号処理部 302 に返送する。例えば、図 7 に示す DES の CBC モード処理構成によれば、 R_a が M_1 、 R_b が M_2 、 ID_{dev} が M_3 に相当し、初期値： $IV = IV_{mem}$ としたときの出力 E_1 、 E_2 、 E_3 が暗号文となる。

暗号文 E_1 、 E_2 、 E_3 を受信した記録再生器 300 の記録再生器暗号処理部 302 は、受信データを認証鍵 K_{ake} で復号化する。受信データの復号化方法は、まず、暗号文 E_1 を認証鍵 K_{ake} で復号化し、その結果と IV_{mem} とを排他的論理和し、乱数 R_a を得る。次に、暗号文 E_2 を認証鍵 K_{ake} で復号化し、その結果と E_1 を排他的論理和し、 R_b を得る。最後に、暗号文 E_3 を認証鍵 K_{ake} で復号化し、その結果と E_2 を排他的論理和し、記録再生器識別情報 ID_{dev} を得る。こうして得られた R_a 、 R_b 、記録再生器識別情報 ID_{dev} の内、 R_b および記録再生器識別情報 ID_{dev} が、記録再生器 300 が送信したものと一致するか検証する。この検証に通った場合、記録再生器 300 の記録再生器暗号処理部 302 は記録デバイス 400 を正当なものとして認証する。

次に、記録再生器 300 の記録再生器暗号処理部 302 は、認証後に使用するセッション鍵 (Session Key (以下、Kses とする)) を生成する (生成方法は、乱数を用いる)。そして、Rb、Ra、Kses の順に、DES の CBC モードで鍵 Kake、初期値 IVmem を用いて暗号化し、記録デバイス 400 の記録デバイス暗号処理部 401 に返送する。

これを受信した記録デバイス 400 の記録デバイス暗号処理部 401 は、受信データを鍵 Kake で復号化する。受信データの復号化方法は、記録再生器 300 の記録再生器暗号処理部 302 における復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた Rb、Ra、Kses の内、Rb および Ra が、記録デバイス 400 が送信したものと一致するか検証する。この検証に通った場合、記録デバイス 400 の記録デバイス暗号処理部 401 は記録再生器 300 を正当なものとして認証する。互いに相手を認証した後は、セッション鍵 Kses は、認証後の秘密通信のための共通鍵として利用される。

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

相互認証に成功した場合には、ステップ S48 からステップ S49 に進み、セッション鍵 Kses を記録再生器 300 の記録再生器暗号処理部 302 で保持するとともに、相互認証が終了したことを示す認証完了フラグをセットする。また、相互認証に失敗した場合には、ステップ S50 に進み、認証処理過程で生成されたセッション鍵 Kses を破棄するとともに、認証完了フラグをクリアする。なお、すでにクリアされている場合には必ずしもクリア処理は必要ではない。

なお、記録デバイス 400 が記録デバイス挿入口から取り除かれた場合には、記録再生器 300 内の記録デバイス検知手段が、記録再生器 300 の制御部 301 に記録デバイス 400 が取り除かれたことを通知し、これを受けた記録再生器 300 の制御部 301 は、記録再生器 300 の記録再生器暗号処理部 302 に対し記録デバイス挿入口番号に対応する認証完了フラグをクリアするように命令し、これを受けた記録再生器 300 の記録再生器暗号処理部 302 は、記録デバイ

ス挿入口番号に対応する認証完了フラグをクリアする。

なお、ここでは相互認証処理を図 13 に示す手続きにしたがって実行する例について説明したが、上述した認証処理例に限らず、例えば先に説明した図 15 の相互認証手続きに従った処理を実行してもよい。また、図 13 に示す手続きにおいて、図 13 の A を記録再生器 300 とし、B を記録デバイス 400 とし、B : 記録デバイス 400 が A : 記録再生器 300 に最初に送付する ID を記録デバイス中の鍵ブロック中の記録デバイス識別情報として相互認証処理を行なってもよい。本発明において実行される認証処理手続きは、様々な処理が適用可能であり、上述の認証処理に限定されるものではない。

(6-2) 相互認証時の鍵ブロックの切り替え

本発明のデータ処理装置における相互認証処理における 1 つの特徴は、記録デバイス 400 側に複数の鍵ブロック (ex. N 個の鍵ブロック) を構成して、記録再生器 300 が 1 つの鍵ブロックを指定 (図 20 の処理フローにおけるステップ S44) して認証処理を実行する点である。先に図 19 において説明したように、記録デバイス 400 の暗号処理部 401 に構成された内部メモリ 405 には複数の鍵ブロックが形成されており、それぞれが異なる鍵データ、ID 情報等各種データを格納している。図 20 で説明した記録再生器 300 と記録デバイス 400 間で実行される相互認証処理は、図 19 の記録デバイス 400 の複数の鍵ブロックの 1 つの鍵ブロックに対して実行される。

従来、記憶媒体とその再生機器間における相互認証処理を実行する構成では、相互認証に用いる鍵 : 認証鍵は共通なものが使用されるのが一般的であった。従って、例えば製品仕向け先 (国別) ごと、あるいは製品ごとに認証鍵を変更しようとする、記録再生器側と、記録デバイス側の認証処理に必要な鍵データを双方の機器において変更することが必要となる。従って例えば新たに発売された記録再生器に格納された認証処理に必要な鍵データは、先に販売された記録デバイスに格納された認証処理に必要な鍵データに対応せず、新たな記録再生器は、古いバージョンの記録デバイスへのアクセスができなくなってしまう

事態が発生する。逆に新しいバージョンの記録デバイスと古いバージョンの記録再生器との関係においても同様の事態が発生する。

本発明のデータ処理装置においては、図19に示すように予め記録デバイス400に複数の異なる鍵セットとしての鍵ブロックが格納されている。記録再生器は例えば製品仕向け先（国別）ごと、あるいは製品、機種、バージョン、アプリケーションごとに、認証処理に適用すべき鍵ブロック、すなわち指定鍵ブロックが設定される。この設定情報は、記録再生器のメモリ部、例えば、図3における内部メモリ307、あるいは、記録再生器300の有するその他の記憶素子内に格納され、認証処理時に図3の制御部301によってアクセスされ設定情報にしたがった鍵ブロック指定が行われる。

記録再生器300の内部メモリ307の記録デバイス認証鍵用マスター鍵MKakeは、それぞれの指定鍵ブロックの設定に従って設定された認証鍵用マスター鍵であり、指定鍵ブロックにのみ対応可能となっており、指定鍵ブロック以外の鍵ブロックとの相互認証は成立しない構成となっている。

図19から理解されるように、記録デバイス400の内部メモリ405には1～NのN個の鍵ブロックが設定され、各鍵ブロック毎に記録デバイス識別情報、認証鍵、初期値、保存鍵、乱数生成鍵、種が格納され、少なくとも認証用のかぎデータがブロック毎に異なるデータとして格納されている。

このように、記録デバイス400の鍵ブロックの鍵データ構成は、ブロック毎に異なっている。従って、例えば、ある記録再生機器Aが内部メモリに格納された記録デバイス認証鍵用マスター鍵MKakeを用いて認証処理を行ない得る鍵ブロックは鍵ブロックNo. 1であり、また別の仕様の記録再生器Bが認証可能な鍵ブロックは別の鍵ブロック、例えば鍵ブロックNo. 2のように設定することが可能となる。

後段でさらに詳細に説明するが、コンテンツを記録デバイス400の外部メモリ402に格納する際、各鍵ブロックに格納された保存鍵Kstrを用いて暗号化処理がなされ、格納されることになる。より、具体的には、コンテンツブロッ

クを暗号化するコンテンツ鍵を保存鍵で暗号化処理する。

図19に示すように保存鍵は、各ブロック毎に異なる鍵として構成されている。従って、異なる鍵ブロックを指定するように設定された2つの異なる設定の記録再生器間においては、ある1つの記録デバイスのメモリに格納されたコンテンツを両方で共通に利用することは防止される。すなわち、異なる設定のなされた記録再生器は、それぞれの設定に合致する記録デバイスに格納されたコンテンツのみが利用できる。

なお、各鍵ブロックについて共通化可能なデータは共通化することも可能であり、例えば認証用の鍵データ、保存鍵データのみを異なるように構成してもよい。

このような記録デバイスに複数の異なる鍵データからなる鍵ブロックを構成する具体例としては、例えば記録再生器300の機種別（据え置き型、携帯型等）で指定すべき鍵ブロック番号を異なるように設定したり、あるいは、アプリケーション毎に指定鍵ブロックを異なるように設定する例がある。さらに、例えば日本で販売する記録再生器については指定鍵ブロックをNo. 1とし、米国で販売する記録再生器は指定鍵ブロックをNo. 2とするように地域ごとに異なる鍵ブロック設定を行なう構成とすることも可能である。このような構成とすることで、それぞれの異なる販売地域で使用され、記録デバイスに異なる保存鍵で格納されたコンテンツは、たとえメモ리카ードのような記録デバイスが米国から日本、あるいは日本から米国へ転送されてきても、異なる鍵設定のなされた記録再生器で利用することは不可能であるので、メモリに格納したコンテンツの不正、無秩序な流通を防止できる。具体的には、異なる保存鍵K s t rで暗号化されているコンテンツ鍵K c o nが2国間で相互に利用可能となる状態を排除することができる。

さらに、図19に示す記録デバイス400の内部メモリ405の鍵ブロック1～Nまでの少なくとも1つの鍵ブロック、例えばNo. Nの鍵ブロックをいずれの記録再生器300においても共通に利用可能な鍵ブロックとして構成してもよ

い。

例えば、全ての機器に鍵ブロックNo. Nとの認証可能な記録デバイス認証鍵用マスター鍵MKakeを格納することで、記録再生器300の機種別、アプリケーション毎、仕向け国毎等に関係なく流通可能なコンテンツとして扱うことができる。例えば、鍵ブロックNo. Nに格納された保存鍵でメモリカードに格納された暗号化コンテンツは、すべての機器において利用可能なコンテンツとなる。例えば、音楽データ等を共通に利用可能な鍵ブロックの保存鍵で暗号化してメモリカードに記憶し、このメモリカードを、やはり共通の記録デバイス認証鍵用マスター鍵MKakeを格納した例えば携帯型の音声再生機器等にセットすることで、メモリカードからのデータの復号再生処理を可能とすることができる。

本発明のデータ処理装置における複数の鍵ブロックを有する記録デバイスの利用例を図21に示す。記録再生器2101は日本向け製品の記録再生器であり、記録デバイスの鍵ブロックのNo. 1, 4との間での認証処理が成立するマスター鍵を持っている。記録再生器2102はUS向け製品の記録再生器であり、記録デバイスの鍵ブロックのNo. 2, 4との間での認証処理が成立するマスター鍵を持っている。記録再生器2103はEU向け製品の記録再生器であり、記録デバイスの鍵ブロックのNo. 3, 4との間での認証処理が成立するマスター鍵を持っている。

例えば記録再生器2101は、記録デバイスA, 2104の鍵ブロック1または鍵ブロック4との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器2102は、記録デバイスB, 2105の鍵ブロック2または鍵ブロック4との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器2103は、記録デバイスC, 2106の鍵ブロック3または鍵ブロック4との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。ここで、記録デバイスA, 2104を記録再生器2

102、または記録再生器2103に装着した場合、鍵ブロック1の保存鍵で暗号処理がなされたコンテンツは、記録再生器2102、記録再生器2103と鍵ブロック1との間での認証が成立しないので利用不可能となる。一方、鍵ブロック4の保存鍵で暗号処理がなされたコンテンツは、記録再生器2102、記録再生器2103と鍵ブロック4との間での認証が成立するので利用可能となる。

上述のように、本発明のデータ処理装置においては、記録デバイスに複数の異なる鍵セットからなる鍵ブロックを構成し、一方、記録再生機器には、特定の鍵ブロックに対する認証可能なマスター鍵を格納する構成としたので、様々な利用態様に応じたコンテンツの利用制限を設定することが可能となる。

なお、1つの記録再生機器において指定可能な鍵ブロックを複数、例えば1～kとし、他の記録再生器において指定可能な鍵ブロックをp～qのように複数とすることも可能であり、また、共通に利用可能な鍵ブロックを複数設ける構成としてもよい。

(7) 記録再生器から記録デバイスへのダウンロード処理

次に、本発明のデータ処理装置において、記録再生器300から記録デバイス400の外部メモリにコンテンツをダウンロードする処理について説明する。

図22は、記録再生器300から記録デバイス400へコンテンツをダウンロードする手順を説明する流れ図である。なお、図22においては、既に記録再生器300と記録デバイス400との間で上述した相互認証処理が完了しているものとする。

ステップS51において、記録再生器300の制御部301は、読み取り部304を使ってコンテンツを格納したメディア500から所定のフォーマットに従ったデータを読み出すか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信する。そして、記録再生器300の制御部301は、データの内のヘッダ(Header)部分(図4参照)を記録再生器300の記録再生器暗号処理部302に送信する。

次に、ステップS52において、ステップS51でヘッダ(Header)を

受信した記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 にチェック値 A を計算させる。チェック値 A は、図 23 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 A 生成鍵 K_{icva} を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図 7 で説明した ICV 計算方法に従って計算される。なお、初期値は、 $IV=0$ としても、記録再生器暗号処理部 302 の内部メモリ 307 にチェック値 A 生成用初期値 IV_a を保存しておき、それを使用してもよい。最後に、チェック値 A とヘッダ (Header) 内に格納されたチェック値: ICV_a を比較し、一致していた場合にはステップ S53 へ進む。

先に図 4 において説明したようにチェック値 A、 ICV_a は、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 A 生成鍵 K_{icva} を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図 7 で説明した ICV 計算方法に従って計算されるチェック値 A が、ヘッダ (Header) 内に格納されたチェック値: ICV_a と一致した場合には、識別情報、取扱方針の改竄はないと判断される。

次に、ステップ S53 において、記録再生器暗号処理部 302 の制御部 306 は、配送鍵 K_{dis} の生成を記録再生器暗号処理部 302 の暗号／復号化部 308 に行わせる。配送鍵 K_{dis} の生成方法としては、例えば次のように生成する。

$$K_{dis} = DES (MK_{dis}, Content\ ID \wedge IV_{dis}) \quad \dots\dots (4)$$

ここで、 MK_{dis} は、配送鍵 K_{dis} を生成するための配送鍵用マスター鍵であり、これは、前述したように記録再生器 300 の内部メモリに格納されてい

る鍵である。またContent IDはコンテンツデータのヘッダ部の識別情報であり、さらにIVdisは、配送鍵用初期値である。また、上記式において、DES () は、第1引数を暗号鍵として、第2引数の値を暗号化する関数であり、演算 \wedge は64ビット単位の排他的論理和を示す。

ステップS54において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308を使って、ステップS53で生成した配送鍵Kdisを用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵Kbitとコンテンツ鍵Kcon (図4参照) の復号化処理を行う。図4に示されるようにこれらブロック情報鍵Kbitとコンテンツ鍵Kconは、DVD、CD等のメディア、あるいはインターネット等の通信路上では、配送鍵Kdisによって予め暗号化処理が施されている。

さらに、ステップS55において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308を使って、ステップS54で復号化したブロック情報鍵Kbitでブロック情報(BIT)を復号化する。図4に示されるようにブロック情報(BIT)は、DVD、CD等のメディア、あるいはインターネット等の通信路上では、ブロック情報鍵Kbitによって予め暗号化処理が施されている。

さらに、ステップS56において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)を8バイト単位に分割し、それら全てを排他的論理和する(加算、減算等、いずれの演算でもよい)。次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にチェック値B(ICVb)を計算させる。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、先ほど計算した排他的論理和値をDESで暗号化して生成する。最後に、チェック値BとHeader内のICVbを比較し、一致していた場合には

ステップS57へ進む。

先に図4において説明したように、チェック値B、ICVbは、ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報(BIT)の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)を8バイト単位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、ヘッダ(Header)内に格納されたチェック値:ICVbと一致した場合には、ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄はないと判断される。

ステップS57において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に中間チェック値の計算をさせる。中間チェック値は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵Kicvtを鍵とし、検証したヘッダ(Header)内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7で説明したICV計算方法に従って計算する。なお、初期値IV=0としても、記録再生器暗号処理部302の内部メモリ307に総チェック値生成用初期値IVtを保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。

この中間チェック値は、チェック値A、チェック値B、全てのコンテンツチェック値をメッセージとして生成されるものであり、これらの各チェック値の検証対象となっているデータについての検証を中間チェック値の照合処理によって行なってもよい。しかし、本実施例においては、システム全体の共有データとしての非改竄性検証処理と、ダウンロード処理後に各記録再生機器300のみが占有する占有データとして識別するための検証処理を区別して実行可能とするために、中間チェック値からさらに複数の異なるチェック値、すなわち総チェック値I

CV t と、記録再生器固有チェック値 I C V d e v とを別々に、中間チェック値に基づいて生成可能としている。これらのチェック値については後段で説明する。

記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に総チェック値 I C V t の計算をさせる。総チェック値 I C V t は、図 2 5 に示すように、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されているシステム署名鍵 K s y s を鍵とし、中間チェック値を D E S で暗号化して生成する。最後に、生成した総チェック値 I C V t とステップ S 5 1 で保存しておいた H e a d e r 内の I C V t を比較し、一致していた場合には、ステップ S 5 8 へ進む。システム署名鍵 K s y s は、複数の記録再生器、すなわちある一定のデータの記録再生処理を実行するシステム集合全体において共通する署名鍵である。

先に図 4 において説明したように、総チェック値 I C V t は、I C V a 、I C V b 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ (H e a d e r) 内に格納されたチェック値 : I C V t と一致した場合には、I C V a 、I C V b 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

次に、ステップ S 5 8 において、記録再生器 3 0 0 の制御部 3 0 1 は、ブロック情報 (B I T) 内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録再生器 3 0 0 の読み取り部 3 0 4 を使ってメディア 5 0 0 から読み出すか、記録再生器 3 0 0 の通信部 3 0 5 を使って通信手段 6 0 0 から受信し、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 へ送信する。これを受信した

記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 にコンテンツ中間値を計算させる。

コンテンツ中間値は、ステップ S 54 で復号化したコンテンツ鍵 K_{con} で、入力されたコンテンツブロックを DES の CBC モードで復号化し、その結果を 8 バイトごとに区切り、全て排他的論理和（加算、減算等、いずれの演算でもよい）して生成する。

次に、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているコンテンツチェック値生成鍵 K_{icvc} を鍵とし、コンテンツ中間値を DES で暗号化して生成する。そして、記録再生器暗号処理部 302 の制御部 306 は、当該コンテンツチェック値と、ステップ S 51 で記録再生器 300 の制御部 301 から受信したコンテンツブロック内の ICV を比較し、その結果を記録再生器 300 の制御部 301 に渡す。これを受信した記録再生器 300 の制御部 301 は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器 300 の記録再生器暗号処理部 302 に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、Header 生成側と合わせておけば、 $IV = 0$ としても、記録再生器暗号処理部 302 の内部メモリ 307 にコンテンツチェック値生成用初期値 IV_c を保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器 300 の記録再生器暗号処理部 302 に保持しておく。さらにまた、記録再生器 300 の記録再生器暗号処理部 302 は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを 2 回以上検証させられたりした場合には、認証に失敗したものとする。そして、全ての検証が成功した場合には、ステップ S 59 へ進む。

次に、ステップ S 59 において、記録再生器 300 の記録再生器暗号処理部 302 は、ステップ S 54 で復号化しておいたブロック情報鍵 K_{bit} とコンテ

ツ鍵K c o nを、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵K s e sで暗号化させる。記録再生器300の制御部301は、セッション鍵K s e sで暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

次に、ステップS60において、記録再生器300から送信されてきたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵K s e sで復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K s t rで再暗号化させる。最後に、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵K s t rで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを読み出す。そして、これらの鍵を、配送鍵K d i sで暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nに置き換える。

ステップS61において、記録再生器300の制御部301は、データのヘッダ部の取扱方針（U s a g e P o l i c y）から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できる（この場合、利用制限情報が1に設定）か、別の同様な記録再生器300でも利用できる（この場合、利用制限情報が0に設定）か判定する。判定の結果、利用制限情報が1であった場合には、ステップS62に進む。

ステップS62において、記録再生器300の制御部301は、記録再生器固有のチェック値を記録再生器300の記録再生器暗号処理部302に計算させる。記録再生器固有のチェック値は、図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている記録再生器署名鍵K d e vを鍵とし、ステップS58で保持しておいた中間チェック値をDESで暗号化して生成する

。計算された記録再生器固有のチェック値 ICV_{dev} は、総チェック値 ICV_t の代わりに上書きされる。

先に説明したように、システム署名鍵 K_{sys} は、配信システムに共通の署名または ICV をつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵 K_{dev} は、記録再生器毎に異なり、記録再生器が署名または ICV をつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵 K_{sys} によって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値 ICV_t が一致することになるので、共通に利用可能となるが、記録再生器署名鍵 K_{dev} を用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵 K_{dev} を用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値 ICV_{dev} が不一致となり、エラーとなるので再生できないことになる。

従って、本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

ステップ $S63$ において、記録再生器 300 の制御部 301 は、コンテンツを記録デバイス 400 の外部メモリ 402 に保存する。

図 26 は、利用制限情報が 0 の場合における記録デバイス内のコンテンツ状況を示す図である。図 27 は、利用制限情報が 1 の場合における記録デバイス内のコンテンツ状況を示す図である。図 26 が図 4 と異なる点は、コンテンツブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} が配送鍵 K_{dis} で暗号化されているか、保存鍵 K_{str} で暗号化されているかだけである。また、図 27 が図 26 と異なる点は、中間チェック値から計算されるチェック値が、図 26 ではシステム署名鍵 K_{sys} で暗号化されているのに対し、図 27 では記録再生器固有の記録再生器署名鍵 K_{dev} で暗号化されていることである。

なお、図 22 の処理フローにおいて、ステップ S 52 でチェック値 A の検証に失敗した場合、ステップ S 56 でチェック値 B の検証に失敗した場合、ステップ S 57 で総チェック値 I C V t の検証に失敗した場合、ステップ S 58 で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合には、ステップ S 64 に進み、所定のエラー表示を行う。

また、ステップ S 61 で利用制限情報が 0 であった場合には、ステップ S 62 をスキップしてステップ S 63 へ進む。

(8) 記録デバイス格納情報の記録再生器での再生処理

次に記録デバイス 400 の外部メモリ 402 に格納されたコンテンツ情報の記録再生器 300 での再生処理について説明する。

図 28 は、記録再生器 300 が記録デバイス 400 からコンテンツを読み出し、コンテンツを利用する手順を説明する流れ図である。なお、図 28 においても、既に記録再生器 300 と記録デバイス 400 との間で相互認証が完了しているものとする。

ステップ S 71 において、記録再生器 300 の制御部 301 は、記録デバイスコントローラ 303 を使って記録デバイス 400 の外部メモリ 402 からコンテンツを読み出す。そして、記録再生器 300 の制御部 301 は、データの内のヘッダ (Header) 部分を記録再生器 300 の記録再生器暗号処理部 302 に送信する。ステップ S 72 は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップ S 52 と同様の処理であり、ヘッダ (Header) を受信した記録再生器暗号処理部 302 の制御部 306 が、記録再生器暗号処理部 302 の暗号／復号化部 308 にチェック値 A を計算させる処理である。チェック値 A は、先に説明した図 23 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 A 生成鍵 K i c v a を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図 7 で説明したと同様の I C V 計算方法に従って計算される。

先に説明したようにチェック値A、ICV aは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K i c v aを鍵とし、識別情報（Content ID）と取扱方針（Usage Policy）をメッセージとして図7で説明したICV計算方法に従って計算されるチェック値Aが、ヘッダ（Header）内に格納されたチェック値：ICV aと一致した場合には、記録デバイス400に格納された識別情報、取扱方針の改竄はないと判断される。

次に、ステップS73において、記録再生器300の制御部301は、読み出したヘッダ（Header）部分からブロック情報鍵K b i tとコンテンツ鍵K c o nを取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。記録再生器300から送信されてきたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K s t rで復号化処理させ、相互認証の際に共有しておいたセッション鍵K s e sで再暗号化させる。そして、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを読み出す。

次に、ステップS74において、記録再生器300の制御部301は、受信したセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを記録再生器300の記録再生器暗号処理部302に送信する。

セッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の暗号／復号化部308に、セッション鍵K s e sで暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを、相互認証の際に

共有しておいたセッション鍵K s e sで復号化させる。そして、復号化したブロック情報鍵K b i tで、ステップS 7 1で受信しておいたブロック情報を復号化させる。

なお、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、復号化したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報B I Tを、ステップS 7 1で受信しておいたブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報B I Tに置き換えて保持しておく。また、記録再生器3 0 0の制御部3 0 1は、復号化されたブロック情報B I Tを記録再生器3 0 0の記録再生器暗号処理部3 0 2から読み出しておく。

ステップS 7 5は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップS 5 6と同様の処理である。記録再生器暗号処理部3 0 2の制御部3 0 6が、記録デバイス4 0 0から読み出したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報(B I T)を8バイト単位に分割し、それら全てを排他的論理和する。次に、記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にチェック値B (I C V b)を計算させる。チェック値Bは、先に説明した図2 4に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値B生成鍵K i c v bを鍵とし、先ほど計算した排他的論理和値をD E Sで暗号化して生成する。最後に、チェック値BとH e a d e r内のI C V bを比較し、一致していた場合にはステップS 7 6へ進む。

先に説明したように、チェック値B, I C V bは、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値B生成鍵K i c v bを鍵とし、記録デバイス4 0 0から読み出したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報(B I T)を8バイト単位に分割し排他的論理和して得られる値をD E Sで暗号化して生成したチェック値Bが、記録デバイス4 0 0から読み出したデータ中のヘッダ(H e a d e r)

内に格納されたチェック値：I C V b と一致した場合には、記録デバイス 4 0 0 に格納されたデータのブロック情報鍵 K b i t、コンテンツ鍵 K c o n、ブロック情報の改竄はないと判断される。

ステップ S 7 6 において、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に中間チェック値の計算をさせる。中間チェック値は、先に説明した図 2 5 に示すように記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されている総チェック値生成鍵 K i c v t を鍵とし、検証したヘッダ (H e a d e r) 内のチェック値 A、チェック値 B、保持しておいた全てのコンテンツチェック値をメッセージとして図 7 他で説明した I C V 計算方法に従って計算する。なお、初期値は $I V = 0$ としても、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に総チェック値生成用初期値に I V t を保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に保持しておく。

次に、ステップ S 7 7 において、記録再生器 3 0 0 の制御部 3 0 1 は、記録デバイス 4 0 0 の外部メモリ 4 0 2 から読み出したデータのヘッダ部に含まれる取扱方針 (U s a g e P o l i c y) から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器 3 0 0 のみで利用できる (利用制限情報が 1) か、別の同様な記録再生器 3 0 0 でも利用できる (利用制限情報が 0) か判定する。判定の結果、利用制限情報が 1、すなわちダウンロードしたコンテンツが当該記録再生器 3 0 0 のみで利用できる利用制限が設定されている場合には、ステップ S 8 0 に進み、利用制限情報が 0、すなわち別の同様な記録再生器 3 0 0 でも利用できる設定であった場合には、ステップ S 7 8 に進む。なお、ステップ S 7 7 の処理は、暗号処理部 3 0 2 が行なってもよい。

ステップ S 7 8 においては、(7) 記録再生器から記録デバイスへのダウンロード処理において説明したステップ S 5 8 と同様の総チェック値 I C V t の計算が実行される。すなわち、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に総チェック値 I C V t の計算

をさせる。総チェック値 ICV_t は、先に説明した図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されているシステム署名鍵 K_{sys} を鍵とし、中間チェック値を DES で暗号化して生成する。

次に、ステップ S 79 に進み、ステップ S 78 において生成した総チェック値 ICV_t とステップ S 71 で保存しておいたヘッダ (Header) 内の ICV_t を比較し、一致していた場合には、ステップ S 82 へ進む。

先に説明したように、総チェック値 ICV_t は、 ICV_a 、 ICV_b 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ (Header) 内に格納されたチェック値： ICV_t と一致した場合には、記録デバイス 400 に格納されたデータにおいて、 ICV_a 、 ICV_b 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

ステップ S 77 での判定において、ダウンロードしたコンテンツが当該記録再生器 300 のみで利用できる設定であった場合、すなわち設定情報が 1 であった場合は、ステップ S 80 に進む。

ステップ S 80 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に、記録再生器固有のチェック値 ICV_{dev} の計算をさせる。記録再生器固有のチェック値 ICV_{dev} は、先に説明した図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されている記録再生器固有の記録再生器署名鍵 K_{dev} を鍵とし、中間チェック値を DES で暗号化して生成する。ステップ S 81 において、ステップ S 80 で計算した記録再生器固有のチェック値 ICV_{dev} とステップ S 71 で保存しておいた Header 内の ICV_{dev} を比較し、一致していた場合には、ステップ S 82 へ進む。

このように、システム署名鍵 K_{sys} によって署名されたデータは、同じシステム署名鍵を有するシステム (記録再生器) によってチェックが成功、すなわち総チェック値 ICV_t が一致することになるので共通に利用可能となり、記録再

生器署名鍵K d e vを用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵K d e vを用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値I C V d e vが不一致となり、エラーとなるので再生できないことになる。従って、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

ステップS 8 2において、記録再生器3 0 0の制御部3 0 1は、ステップS 7 4で読み出しておいたブロック情報B I T内のコンテンツブロック情報を取り出し、コンテンツブロックが暗号化対象になっているかいないか調べる。暗号化対象になっていた場合には、該当するコンテンツブロックを、記録再生器3 0 0の記録デバイスコントローラ3 0 3を介し、記録デバイス4 0 0の外部メモリ4 0 2から読み出し、記録再生器3 0 0の記録再生器暗号処理部3 0 2へ送信する。これを受信した記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にコンテンツを復号化させるとともに、コンテンツブロックが検証対象になっている場合には次のステップS 8 3においてコンテンツチェック値を検証させる。

ステップS 8 3は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップS 5 8と同様の処理である。記録再生器3 0 0の制御部3 0 1は、ブロック情報(B I T)内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないかをコンテンツチェック値の格納状況から判定し、コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録デバイス4 0 0の外部メモリ4 0 2から受信し、記録再生器3 0 0の記録再生器暗号処理部3 0 2へ送信する。これを受信した記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にコンテンツ中間値を計算させる。

コンテンツ中間値は、ステップS 7 4で復号化したコンテンツ鍵K c o nで、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を8バイトに区切り全て排他的論理和して生成する。

次に、記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているコンテンツチェック値生成鍵K i c v cを鍵とし、コンテンツ中間値をDESで暗号化して生成する。そして、記録再生器暗号処理部3 0 2の制御部3 0 6は、当該コンテンツチェック値と、ステップS 7 1で記録再生器3 0 0の制御部3 0 1から受信したコンテンツブロック内のICVを比較し、その結果を記録再生器3 0 0の制御部3 0 1に渡す。これを受信した記録再生器3 0 0の制御部3 0 1は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器3 0 0の記録再生器暗号処理部3 0 2に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、初期値はIV=0としても、記録再生器暗号処理部3 0 2の内部メモリ3 0 7にコンテンツチェック値生成用初期値IVcを保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器3 0 0の記録再生器暗号処理部3 0 2に保持しておく。さらにまた、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上検証させられたりした場合には、認証に失敗したものとする。

記録再生器3 0 0の制御部3 0 1は、当該コンテンツチェック値の比較結果（検証対象になっていない場合、比較結果は全て成功とする）を受信し、検証に成功していた場合には、記録再生器3 0 0の記録再生器暗号処理部3 0 2から復号化されたコンテンツを取り出す。そして、次の復号化対象コンテンツブロックを取り出して記録再生器3 0 0の記録再生器暗号処理部3 0 2に復号化させ、全てのコンテンツブロックを復号化するまで繰り返す。

なお、ステップS 8 3において、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、コンテンツチェック値の検証処理において不一致となった場合には、検証失敗としてその時点で処理を中止し、残るコンテンツの復号化は行わない。また、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、復号化対象のコンテンツブロックの復号化順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上復号化させられたりした場合には、復号化に失敗したものとする。

なお、ステップS 7 2でチェック値Aの検証に失敗した場合、ステップS 7 5でチェック値Bの検証に失敗した場合、ステップS 7 9で総チェック値ICV_tの検証に失敗した場合、ステップS 8 1で記録再生器固有のチェック値ICV_de_vの検証に失敗した場合には、ステップS 8 3で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合、ステップS 8 4に進み、所定のエラー表示を行う。

以上説明してきたように、コンテンツをダウンロードしたり、利用したりする際に、重要なデータやコンテンツを暗号化しておいて隠蔽化したり、改竄検証ができるだけでなく、ブロック情報BITを復号化するためのブロック情報鍵K_bi_t、コンテンツを復号化するためのコンテンツ鍵K_co_nが記録デバイス固有の保存鍵K_st_rで保存されているため、単純に記録メディア上のデータを別の記録メディアに複製したとしても、コンテンツを正しく復号化することができなくすることができる。より具体的には、例えば図28のステップS 7 4において、記録デバイス毎に異なる保存鍵K_st_rで暗号化されたデータを復号化するため、別の記録デバイスではデータを正しく復号化できない構成を持つからである。

(9) 相互認証後の鍵交換処理

本発明のデータ処理装置における特徴の1つに、上述した記録再生器3 0 0と記録デバイス4 0 0との間で実行される相互認証処理の後においてのみ、記録デバイスの利用を可能とし、また、その利用態様を制限した点がある。

例えば、不正な複製等によってコンテンツを格納したメモリカード等の記録デバイスを生成し、これを記録再生器にセットして利用されることを排除するために、記録再生器300と、記録デバイス400間での相互認証処理を実行し、かつ認証OKとなったことを条件として、コンテンツ（暗号化された）の記録再生器300および記録デバイス400間での転送を可能としている。

上記の制限的処理を実現するために、本発明のデータ処理装置においては、記録デバイス400の暗号処理部401での処理は、すべて、予め設定されたコマンド列に基づいて実行される構成となっている。すなわち、記録デバイスは、コマンド番号に基づくコマンドを順次レジスタから取り出して実行するコマンド処理構成を持つ。この記録デバイスでのコマンド処理構成を説明する図を図29に示す。

図29に示すように記録再生器暗号処理部302を有する記録再生器300と記録デバイス暗号処理部401を有する記録デバイス400間においては、記録再生器300の制御部301の制御のもとに記録デバイスコントローラ303から記録デバイス400の通信部(受信レジスタを含む)404に対してコマンド番号(N o .)が出力される。

記録デバイス400は、暗号処理部401内の制御部403にコマンド番号管理部2201を有する。コマンド番号管理部2901は、コマンドレジスタ2902を保持しており、記録再生器300から出力されるコマンド番号に対応するコマンド列を格納している。コマンド列は、図29の右に示すようにコマンド番号0からyまで順次、コマンド番号に対して実行コマンドが対応付けされている。コマンド番号管理部2901は、記録再生器300から出力されるコマンド番号を監視し、対応するコマンドをコマンドレジスタ2902から取り出して実行する。

コマンドレジスタ2902に格納されたコマンドシーケンスは、図29の右に示すように、認証処理シーケンスに関するコマンド列が先行するコマンド番号0～kに対応付けられている。さらに、認証処理シーケンスに関するコマンド列の

後のコマンド番号 p ～ s に復号、鍵交換、暗号処理コマンドシーケンス 1、さらに、後続するコマンド番号 u ～ y に復号、鍵交換、暗号処理コマンドシーケンス 2 が対応付けされている。

先に図 20 の認証処理フローにおいて説明したように、記録デバイス 400 が記録再生器 300 に装着されると、記録再生器 300 の制御部 301 は、記録デバイスコントローラ 303 を介して記録デバイス 400 に初期化命令を送信する。これを受信した記録デバイス 400 は、記録デバイス暗号処理部 401 の制御部 403 において、通信部 404 を介して命令を受信し、認証フラグ 2903 をクリアする。すなわち未認証状態に設定する。または、記録再生器 300 から記録デバイス 400 に電源が供給される様な場合には、パワーオン時に未承認状態としてセットを行なう方式でもよい。

次に、記録再生器 300 の制御部 301 は、記録再生器暗号処理部 302 に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器 300 に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス 400 との認証処理、およびデータ送受信が可能となる。

初期化命令を受信した記録再生器 300 の記録再生器暗号処理部 302 は、記録再生器暗号処理部 302 の制御部において、記録デバイス挿入口番号に対応する認証フラグ 2904 をクリアする。すなわち未認証状態に設定する。

これらの初期化処理が完了すると、記録再生器 300 の制御部 301 は、記録デバイスコントローラ 303 を介してコマンド番号 0 から順次コマンド番号を昇順に出力する。記録デバイス 400 のコマンド番号管理部 2901 は、記録再生器 300 から入力されるコマンド番号を監視し、0 から順次入力されることを確認して、対応するコマンドをコマンドレジスタ 2902 から取り出して認証処理等各種処理を実行する。入力されるコマンド番号が規定の順でなかった場合には、エラーとし、コマンド番号受付値を初期状態、すなわち実行可能コマンド番号 = 0 にリセットする。

図 29 に示すようにコマンドレジスタ 2902 に格納されたコマンドシーケンスは、認証処理を先行して処理するようにコマンド番号が付与されており、その後の処理に復号、鍵交換、暗号化処理の処理シーケンスが格納されている。

復号、鍵交換、暗号化処理の処理シーケンスの具体例を図 30, 31 を用いて説明する。

図 30 は、先に図 22 において説明した記録再生器 300 から記録デバイス 400 へのコンテンツのダウンロード処理において実行される処理の一部を構成するものである。具体的には図 22 におけるステップ S59 ~ S60 の間で実行される

図 30 において、ステップ S3001 は、記録再生器からセッション鍵 K_{ses} で暗号化されたデータ (ex. ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con}) を記録デバイスが受信する処理であり、その後、前述の図 29 で示したコマンド列 $p \sim s$ が開始される。コマンド列 $p \sim s$ は認証処理コマンド 0 ~ k が完了し、図 29 に示す認証フラグ 2903, 2904 に認証済みのフラグがセットされた後開始される。これは、コマンド番号管理部 2901 がコマンド番号を 0 から昇順でのみ受け付けることによって保証される。

ステップ S3002 は、記録デバイスが記録再生器から受信したセッション鍵 K_{ses} で暗号化されたデータ (ex. ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con}) をレジスタに格納する処理である。

ステップ S3003 は、セッション鍵 K_{ses} で暗号化されたデータ (ex. ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con}) をレジスタから取り出してセッション鍵 K_{ses} で復号する処理を実行するステップである。

ステップ S3004 は、セッション鍵 K_{ses} で復号化されたデータ (ex. ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con}) を保存鍵 K_{str} で暗号化する処理を実行するステップである。

上記の処理ステップ 3002 ~ 3004 は、先の図 29 で説明したコマンドレジスタ中のコマンド番号 $p \sim s$ に含まれる処理である。これらの処理は、記録デ

バイス400のコマンド番号管理部2901において記録再生器300から受信するコマンド番号p～sに従って記録デバイス暗号処理部401が順次実行する。

次のステップS3005は、保存鍵Kstrで暗号化したデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）を記録デバイスの外部メモリに格納するステップである。このステップにおいては、記録デバイス暗号処理部401から記録再生器300が保存鍵Kstrで暗号化したデータを読み出して、その後記録デバイス400の外部メモリ402に格納してもよい。

上述のステップS3002～S3004は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップS3003の復号処理終了時点で、記録再生器300からのデータ読み出し命令があつたとしても、その読み出しコマンドは、コマンドレジスタ2902のコマンド番号p～sに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部2901は、読み出しの実行を受け付けない。従って、記録デバイス400における鍵交換の際に発生する復号データを外部、例えば記録再生器300から読み出すことは不可能となり、鍵データ、コンテンツの不正な読み出しを防止できる。

図31は、先に図28において説明した記録デバイス400からコンテンツを読み出して記録再生器300において再生するコンテンツ再生処理において実行される処理の一部を構成するものである。具体的には図28におけるステップS73において実行される処理である。

図31において、ステップS3101は、記録デバイス400の外部メモリ402から保存鍵Kstrで暗号化されたデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）の読み出しを実行するステップである。

ステップS3102は、記録デバイスのメモリから読み出した保存鍵Kstrで暗号化されたデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）をレジスタに格納するステップである。このステップにおいては、記録デバイス400の外部メモリ402から記録再生器300が保存鍵Kstrで暗号化し

たデータを読み出して、その後に記録デバイス400のレジスタに格納してもよい。

ステップS3103は、保存鍵K_{s t r}で暗号化されたデータ（e x. ブロック情報鍵K_{b i t}、コンテンツ鍵K_{c o n}）をレジスタから取り出して保存鍵K_{s t r}で復号処理するステップである。

ステップS3104は、保存鍵K_{s t r}で復号化されたデータ（e x. ブロック情報鍵K_{b i t}、コンテンツ鍵K_{c o n}）をセッション鍵K_{s e s}で暗号化処理するステップである。

上記の処理ステップ3102～3104は、先の図29で説明したコマンドレジスタ中のコマンド番号u～yに含まれる処理である。これらの処理は、記録デバイスのコマンド番号管理部2901において記録再生器300から受信するコマンド番号u～yに従って記録デバイス暗号処理部406が順次実行する。

次のステップS3105は、セッション鍵K_{s e s}で暗号化したデータ（e x. ブロック情報鍵K_{b i t}、コンテンツ鍵K_{c o n}）を記録デバイスから記録再生器へ送信する処理である。

上述のステップS3102～S3104は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップS3103の復号処理終了時点で、記録再生器300からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ2902のコマンド番号u～yに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部2901は、読み出しの実行を受け付けない。従って、記録デバイス400における鍵交換の際に発生する復号データを外部、例えば記録再生器300から読み出すことは不可能となり、鍵データあるいはコンテンツの不正な読み出しを防止できる。

なお、図30、31に示す処理では、鍵交換によって復号、暗号化される対象が、ブロック情報鍵K_{b i t}、コンテンツ鍵K_{c o n}である例を示したが、これらの図29に示したコマンドレジスタ2902に格納されたコマンドシーケンスには、コンテンツ自体の鍵交換を伴う復号、暗号化処理を含ませてもよく、鍵交

換によって復号、暗号化される対象は上述の例に限定されるものではない。

以上、本発明のデータ処理装置における相互認証後の鍵交換処理について説明した。このように、本発明のデータ処理装置における鍵交換処理は、記録再生器と記録デバイス間での認証処理が終了した後においてのみ実行可能となり、さらに、鍵交換処理における復号データの外部からのアクセスが防止可能な構成となっているので、コンテンツ、鍵データの高度なセキュリティが確保される。

(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理

上述した実施例では、例えば図3に示すメディア500あるいは通信手段600におけるデータフォーマットが図4に示す1つの種類である場合について説明してきた。しかしながら、メディア500あるいは、通信手段600におけるデータフォーマットは、上述の図4に示すフォーマットに限らず、コンテンツが音楽である場合、画像データである場合、ゲーム等のプログラムである場合等、コンテンツに応じたデータフォーマットを採用することが望ましい。以下、複数の異なるデータデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理について説明する。

図32～35に4つの異なるデータフォーマットを示す。各図の左側には、図3に示すメディア500、または通信手段600上におけるデータフォーマットを、また各図の右側には記録デバイス400の外部メモリ402に格納される場合のデータフォーマットを示してある。先に、図32～35に示すデータフォーマットの概略を説明し、その後、各フォーマットにおける各データの内容、および各フォーマットにおけるデータの差異について説明する。

図32は、フォーマットタイプ0であり、上述の説明中で例として示したタイプと共通のものである。このフォーマットタイプ0の特徴は、データ全体を任意の大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割し、各ブロックについて任意に暗号化し、暗号化ブロックと非暗号化ブロック、すなわち平文ブロックを混在させてデータを構成できる点である。ブロックの暗号化

は、コンテンツ鍵K c o nによって実行されており、コンテンツ鍵K c o nは、メディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。ブロック情報鍵K b i tについてもメディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。これらの鍵交換は、前述の「(9) 相互認証後の鍵交換処理」において説明した処理にしたがって実行される。

図33は、フォーマットタイプ1であり、このフォーマットタイプ1は、フォーマットタイプ0と同様、データ全体をN個のデータブロック、すなわちブロック1～ブロックNに分割しているが、N個の各ブロックの大きさを同じ大きさとした点で前述のフォーマットタイプ0と異なる。コンテンツ鍵K c o nによるブロックの暗号化処理態様は前述のフォーマットタイプ0と同様である。また、メディア上で配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化されるコンテンツ鍵K c o nおよびブロック情報鍵K b i t構成も上述のフォーマットタイプ0と同様である。フォーマットタイプ1は、フォーマットタイプ0と異なり、固定的なブロック構成としたことで、ブロック毎のデータ長等の構成データが簡略化されるので、フォーマットタイプ0に比較してブロック情報のメモリサイズを減らすことが可能となる。

図33の構成例では、各ブロックを暗号化パートと非暗号化（平文）パートの1組によって構成している。このようにブロックの長さ、構成が規則的であれば、復号処理等の際に各ブロック長、ブロック構成を確認する必要がなくなるので効率的な復号、暗号処理が可能となる。なお、フォーマット1においては、各ブロックを構成するパート、すなわち暗号化パート、非暗号化（平文）パートは、各パート毎にチェック対象として定義可能な構成となっており、要チェックパーツを含むブロックである場合は、そのブロックに関してコンテンツチェック値I

C V i が定義される。

図34は、フォーマットタイプ2であり、このフォーマットタイプ2の特徴は、同じ大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割され、各ブロックについて、それぞれ個別のブロック鍵K b l c で暗号化されていることである。各ブロック鍵K b l c の暗号化は、コンテンツ鍵K c o n によって実行されており、コンテンツ鍵K c o n は、メディア上では配送鍵K d i s によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t r によって暗号化される。ブロック情報鍵K b i t についてもメディア上では配送鍵K d i s によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t r によって暗号化される。

図35は、フォーマットタイプ3であり、このフォーマットタイプ3の特徴は、フォーマット・タイプ2と同様、同じ大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割され、各ブロックについて、それぞれ個別のブロック鍵K b l c で暗号化されていること、さらに、コンテンツ鍵を用いず、各ブロック鍵K b l c の暗号化は、メディア上では配送鍵K d i s によって暗号化され、記録デバイス上では保存鍵K s t r によって暗号化されている点である。コンテンツ鍵K c o n は、メディア上、デバイス上、いずれにも存在しない。ブロック情報鍵K b i t はメディア上では配送鍵K d i s によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t r によって暗号化される。

次に、上記フォーマットタイプ0～3のデータの内容について説明する。データは先に説明したように、ヘッダ部とコンテンツ部に大きく2つに分類され、ヘッダ部にはコンテンツ識別子、取扱方針、チェック値A, B, 総チェック値、ブロック情報鍵、コンテンツ鍵、ブロック情報が含まれる。

取扱方針には、コンテンツのデータ長、ヘッダ長、フォーマットタイプ（以下説明するフォーマット0～3）、例えばプログラムであるか、データであるか等

のコンテンツタイプ、前述のコンテンツの記録デバイスへのダウンロード、再生の欄で説明したように、コンテンツが記録再生器固有に利用可能か否かを決定するフラグであるローカリゼーション・フラグ、さらに、コンテンツのコピー、ムーブ処理に関する許可フラグ、さらに、コンテンツ暗号化アルゴリズム、モード等、コンテンツに関する各種の利用制限情報および処理情報を格納する。

チェック値A：I C V aは、識別情報、取扱方針に対するチェック値であり、例えば、前述の図23で説明した手法によって生成される。

ブロック情報鍵K b i tは、ブロック情報を暗号化するための鍵であり、先に説明したように、メディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。

コンテンツ鍵K c o nは、コンテンツの暗号化に用いる鍵であり、フォーマットタイプ0, 1では、ブロック情報鍵K b i tと同様にメディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。なお、フォーマットタイプ2では、コンテンツ鍵K c o nは、コンテンツ各ブロックに構成されるブロック鍵K b l cの暗号化にも利用される。また、フォーマット・タイプ3においては、コンテンツ鍵K c o nは存在しない。

ブロック情報は、個々のブロックの情報を記述するテーブルであり、ブロックの大きさ、暗号化されているか否かについてのフラグ、すなわち各ブロックがチェックの対象（I C V）と、なっているか否かを示す情報が格納される。ブロックがチェックの対象となっている場合は、ブロックのチェック値I C V i（ブロックiのチェック値）がテーブル中に定義されて格納される。このブロック情報は、ブロック情報暗号鍵K b i tによって暗号化される。

なお、ブロックのチェック値、すなわちコンテンツチェック値I C V iは、ブロックが暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値を記録再生器300の内部メモリ307に格納されたコンテンツチェッ

ク値生成鍵 K_{icvc} で暗号化した値として生成される。また、ブロックが暗号化されていない場合は、ブロックデータ（平文）の全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。図36にコンテンツブロックのチェック値 ICV_i を生成する構成例を示す。メッセージ M の各々が復号文データまたは平文データの各8バイトを構成する。

なお、フォーマット・タイプ1においては、ブロック内のパーツのうち少なくとも1つがチェック値 ICV_i の対象データ、すなわち要チェックパーツである場合は、そのブロックに関してコンテンツチェック値 ICV_i が定義される。ブロック i におけるパーツ j のチェック値 $P-ICV_{ij}$ は、パーツ j が暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値をコンテンツチェック値生成鍵 K_{icvc} で暗号化した値として生成される。また、パーツ j が暗号化されていない場合は、パーツのブロックのデータ（平文）の全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。

さらに、1つのブロック i 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツ、すなわち要チェックパーツが1つのみ存在する場合は、上述の手法で生成したチェック値 $P-ICV_{ij}$ をそのままブロックのチェック値 ICV_i とし、また、1つのブロック i 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが複数存在する場合は、複数のパーツチェック値 $P-ICV_{ij}$ をパーツ番号順に連結したデータを対象にして8バイト単位で図37に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。図37にコンテンツブロックのコンテンツチェック値 ICV_i を生成する構成例を示す。

なお、フォーマット・タイプ2, 3においては、ブロックのチェック値 ICV

i は定義されない。

チェック値 B : I C V b は、ブロック情報鍵、コンテンツ鍵、ブロック情報全体に対するチェック値であり、例えば、前述の図 2 4 で説明した手法によって生成される。

総チェック値 I C V t は、前述のチェック値 A : I C V a、チェック値 B : I C V b、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 I C V i 全体に対するチェック値であり、前述の図 2 5 で説明したようにチェック値 A : I C V a 等の各チェック値から生成される中間チェック値にシステム署名鍵 K s y s を適用して暗号化処理を実行することによって生成される。

なお、フォーマット・タイプ 2, 3 においては、総チェック値 I C V t は、前述のチェック値 A : I C V a、チェック値 B : I C V b にコンテンツデータ、すなわちブロック 1 のブロック鍵から最終ブロックまでのコンテンツデータ全体を連結したデータから生成される中間チェック値にシステム署名鍵 K s y s を適用して暗号化処理を実行することによって生成される。図 3 8 にフォーマット・タイプ 2, 3 における総チェック値 I C V t を生成する構成例を示す。

固有チェック値 I C V d e v は、前述のローカリゼーションフラグが 1 にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 I C V t に置き換えられるチェック値であり、フォーマット・タイプ 0, 1 の場合は、前述のチェック値 A : I C V a、チェック値 B : I C V b、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 I C V i 全体に対するチェック値として生成される。具体的には、前述の図 2 5、または図 3 8 で説明したようにチェック値 A : I C V a 等の各チェック値から生成される中間チェック値に記録再生器署名鍵 K d e v を適用して暗号化処理を実行することによって生成される。

次にフォーマットタイプ 0 ~ 3 各々における記録再生器 3 0 0 から記録デバイス 4 0 0 に対するコンテンツのダウンロード処理、および記録再生器 3 0 0 にお

ける記録デバイス400からの再生処理について図39～44のフローを用いて説明する。

まず、フォーマットタイプ0, 1におけるコンテンツのダウンロード処理について図39を用いて説明する。

図39に示す処理は、例えば図3に示す記録再生器300に記録デバイス400を装着することによって開始される。ステップS101は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図20の認証処理フローに従って実行される。

ステップS101の認証処理が終了し、認証フラグがセットされると、記録再生器300は、ステップS102において、例えばコンテンツデータを格納したメディア500から、読み取り部304を介して所定のフォーマットに従ったデータを読み出すか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信し、記録再生器300の制御部301が、データの内のヘッダ (Header) 部分を記録再生器300の記録再生器暗号処理部302に送信する。

次に、ステップS103において、暗号処理部302の制御部306が記録再生器暗号処理部302の暗号／復号化部308にチェック値Aを計算させる。チェック値Aは、図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵Kicvaを鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図7を用いて説明したICV計算方法に従って計算される。次に、ステップS104において、チェック値Aとヘッダ (Header) 内に格納されたチェック値: ICVaを比較し、一致していた場合にはステップS105へ進む。

先に説明したようにチェック値A, ICVaは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵Kicvaを鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージ

として、例えばICV計算方法に従って計算されるチェック値Aが、ヘッダ（Header）内に格納されたチェック値：ICVaと一致した場合には、識別情報、取扱方針の改竄はないと判断される。

次に、ステップS105において、記録再生器暗号処理部302の制御部306は、配送鍵Kdisの取り出しまたは生成を記録再生器暗号処理部302の暗号／復号化部308に行わせる。配送鍵Kdisの生成方法は、先に説明した図22のステップS53と同様、例えば配送鍵用マスター鍵MKdisを用いて行われる。

次にステップS106において、記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号／復号化部308を使って、生成した配送鍵Kdisを用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵Kbitとコンテンツ鍵Kconの復号化処理を行う。

さらに、ステップS107において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308において、復号化したブロック情報鍵Kbitでブロック情報を復号化する。

さらに、ステップS108において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報（BIT）から、チェック値B（ICVb'）を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報（BIT）からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ（Header）内のICVbを比較し、一致していた場合にはステップS110へ進む。

先に説明したように、チェック値B、ICVbは、ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄を検証するためのチェック値である

。記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 B 生成鍵 K_{icvb} を鍵とし、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} およびブロック情報 (BIT) を 8 バイト単位に分割し排他的論理和して得られる値を DES で暗号化して生成したチェック値 B が、ヘッダ (Header) 内に格納されたチェック値: ICV_b と一致した場合には、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} 、ブロック情報の改竄はないと判断される。

ステップ S110 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に中間チェック値の計算をさせる。中間チェック値は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されている総チェック値生成鍵 K_{icvt} を鍵とし、検証した Header 内のチェック値 A、チェック値 B、保持しておいた全てのコンテンツチェック値をメッセージとして図 7 他で説明した ICV 計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器 300 の記録再生器暗号処理部 302 に保持しておく。

次に、ステップ S111 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に総チェック値 ICV_t' の計算をさせる。総チェック値 ICV_t' は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているシステム署名鍵 K_{sys} を鍵とし、中間チェック値を DES で暗号化して生成する。次に、ステップ S112 において、生成した総チェック値 ICV_t' とヘッダ (Header) 内の ICV_t を比較し、一致していた場合には、ステップ S113 へ進む。

先に図 4 において説明したように、総チェック値 ICV_t は、 ICV_a 、 ICV_b 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ (Header) 内に格納されたチェック値: ICV_t と一致した場合には、 ICV_a 、 ICV_b 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

次に、ステップS 1 1 3において、記録再生器3 0 0の制御部3 0 1は、ブロック情報（B I T）内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

コンテンツブロックが検証対象になっていた場合には、ステップS 1 1 4において、該当するコンテンツブロックを、記録再生器3 0 0の読み取り部3 0 4を使ってメディア5 0 0から読み出すか、記録再生器3 0 0の通信部3 0 5を使って通信手段6 0 0から受信し、記録再生器3 0 0の記録再生器暗号処理部3 0 2へ送信する。これを受信した記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8にコンテンツチェック値I C V i' を計算させる。

コンテンツチェック値I C V i' は、先に説明したようにブロックが暗号化されている場合、コンテンツ鍵K c o nで、入力されたコンテンツブロックをD E SのC B Cモードで復号化し、その結果を全て8バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器3 0 0の内部メモリ3 0 7に格納されたコンテンツチェック値生成鍵K i c v cで暗号化して生成する。また、ブロックが暗号化されていない場合は、データ（平文）全体を8バイト単位で図3 6に示す改竄チェック値生成関数（D E S－C B C－M A C、コンテンツチェック値生成鍵K i c v cを鍵とする）に入力して得た値として生成される。

次にステップS 1 1 5において、記録再生器暗号処理部3 0 2の制御部3 0 6は、当該コンテンツチェック値と、ステップS 1 0 2で記録再生器3 0 0の制御部3 0 1から受信したコンテンツブロック内のI C Vを比較し、その結果を記録再生器3 0 0の制御部3 0 1に渡す。これを受信した記録再生器3 0 0の制御部3 0 1は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器3 0 0の記録再生器暗号処理部3 0 2に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す（ステップS 1 1 6）。

なお、ステップS104、ステップS109、ステップS112、ステップS115のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとしてダウンロード処理は終了する。

次に、ステップS117において、記録再生器300の記録再生器暗号処理部302は、ステップS106で復号化したブロック情報鍵Kbitとコンテンツ鍵Kconを、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵Ksesで暗号化させる。記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

次に、ステップS118において、記録再生器300から送信されてきたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再び暗号化させ、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵Kstrで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを読み出す。すなわち、配送鍵Kdisで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconの鍵のかけかえを行なう。

次に、ステップS119において、記録再生器300の制御部301は、データのヘッダ部の取扱方針(Usage Policy)から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できるか否かの判定を行なう。この判定は、ローカリゼーションフラグ(利用制限情報)=1に設定されている場合は、ダウンロードしたコンテンツが当該記録再生器300のみで利用でき、ローカリゼーションフラグ(利用制限情報)=0に設定さ

れている場合は、ダウンロードしたコンテンツが別の同様な記録再生器 300 でも利用できることを示す。判定の結果、ローカリゼーションフラグ（利用制限情報）＝1であった場合には、ステップ S120 に進む。

ステップ S120 において、記録再生器 300 の制御部 301 は、記録再生器固有のチェック値を記録再生器 300 の記録再生器暗号処理部 302 に計算させる。記録再生器固有のチェック値は、図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されている記録再生器に固有の記録再生器署名鍵 K_{dev} を鍵とし、ステップ S110 で生成した中間チェック値を DES で暗号化して生成する。計算された記録再生器固有のチェック値 ICV_{dev} は、総チェック値 ICV_t の代わりに上書きされる。

先に説明したように、システム署名鍵 K_{sys} は、配信システムに共通の署名または ICV をつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵 K_{dev} は、記録再生器毎に異なり、記録再生器が署名または ICV をつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵 K_{sys} によって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値 ICV_t が一致することになるので、共通に利用可能となるが、記録再生器署名鍵 K_{dev} を用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵 K_{dev} を用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装置して再生しようとした場合、記録再生器固有のチェック値 ICV_{dev} が不一致となり、エラーとなるので再生できないことになる。本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定できるものである。

次に、ステップ S121 において、記録再生器 300 の制御部 301 は、記録再生器暗号処理部 302 に格納データフォーマットの形成を実行させる。先に説明したように、フォーマットタイプは 0～3 まで各タイプがあり、ヘッダ中の取

扱方針（図 5 参照）中に設定され、この設定タイプにしたがって、先に説明した図 3 2～3 5 の右側の格納フォーマットにしたがってデータを形成する。この図 3 9 に示すフローはフォーマット 0, 1 のいずれかであるので、図 3 2, 3 3 のいずれかのフォーマットに形成される。

ステップ S 1 2 1 において格納データフォーマットの形成が終了すると、ステップ 1 2 2 において、記録再生器 3 0 0 の制御部 3 0 1 は、コンテンツを記録デバイス 4 0 0 の外部メモリ 4 0 2 に保存する。

以上が、フォーマットタイプ 0, 1 におけるコンテンツデータのダウンロード処理の態様である。

次に、フォーマットタイプ 2 におけるコンテンツデータのダウンロード処理について図 4 0 を用いて説明する。上記したフォーマットタイプ 0, 1 のダウンロード処理と異なる点を中心に説明する。

ステップ S 1 0 1～S 1 0 9 は、上記したフォーマットタイプ 0, 1 のダウンロード処理と同様であるので説明は省略する。

フォーマットタイプ 2 は、先に説明したようにコンテンツチェック値 ICV_i が定義されていないので、ブロック情報中には、コンテンツチェック値 ICV_i を持たない。フォーマットタイプ 2 における中間チェック値は、図 3 8 に示すようにチェック値 A、チェック値 B と、第 1 ブロックの先頭データ（ブロック 1 のブロック鍵）から最終ブロックまでのコンテンツデータ全体を連結したデータに基づいて生成される中間チェック値にシステム署名鍵 K_{sys} を適用して暗号化処理を実行することによって生成される。

従って、フォーマットタイプ 2 のダウンロード処理においては、ステップ S 1 5 1 においてコンテンツデータを読み出し、ステップ S 1 5 2 において、チェック値 A、チェック値 B と読み出したコンテンツデータに基づいて中間チェック値の生成を実行する。なお、コンテンツデータは暗号化されている場合でも、復号処理を行なわない。

フォーマットタイプ 2 では、前述のフォーマットタイプ 0, 1 での処理のよう

にブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となる。

ステップS 1 1 1 以下の処理は、フォーマットタイプ0, 1における処理と同様であるので説明を省略する。

以上が、フォーマットタイプ2におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ2のダウンロード処理は、フォーマットタイプ0, 1での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

次に、フォーマットタイプ3におけるコンテンツデータのダウンロード処理について図41を用いて説明する。上記したフォーマットタイプ0, 1, 2のダウンロード処理と異なる点を中心に説明する。

ステップS 1 0 1 ~ S 1 0 5 は、上記したフォーマットタイプ0, 1, 2のダウンロード処理と同様であるので説明は省略する。

フォーマットタイプ3は、基本的にフォーマットタイプ2における処理と共通する部分が多いが、フォーマットタイプ3はコンテンツ鍵を有しておらず、またブロック鍵K b 1 c が記録デバイスにおいては保存鍵K s t r で暗号化されて格納される点がフォーマットタイプ2と異なる。

フォーマットタイプ3のダウンロード処理におけるフォーマットタイプ2と相違する点を中心として説明する。フォーマットタイプ3では、ステップS 1 0 5 の次ステップであるステップS 1 6 1 において、ブロック情報鍵の復号を行なう。記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号／復号化部308を使って、ステップS 1 0 5 で生成した配送鍵K d i s を用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵K b i t の復号化処理を行う。フォーマットタイプ3では、データ中にコンテンツ鍵K c o n が存在しないため、コンテンツ鍵K c o n の復号化処理

は実行されない。

次のステップS107では、ステップS161で復号したブロック情報鍵Kbitを用いてブロック情報の復号が実行され、さらに、ステップS162において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵Kbit、およびブロック情報（BIT）から、チェック値B（ICVb'）を生成する。チェック値Bは、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、およびブロック情報（BIT）からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ（Header）内のICVbを比較し、一致していた場合にはステップS151へ進む。

フォーマットタイプ3では、チェック値B、ICVbは、ブロック情報鍵Kbit、ブロック情報の改竄を検証するためのチェック値として機能する。生成したチェック値Bが、ヘッダ（Header）内に格納されたチェック値：ICVbと一致した場合には、ブロック情報鍵Kbit、ブロック情報の改竄はないと判断される。

ステップS151～S112は、フォーマットタイプ2の処理と同様であるので説明を省略する。

ステップS163では、ステップS151で読み出したコンテンツデータに含まれるブロック鍵KblcをステップS105で生成した配送鍵Kdisによって復号する。

次にステップS164では、記録再生器300の記録再生器暗号処理部302が、ステップS161で復号化したブロック情報鍵Kbitと、ステップS163で復号したブロック鍵Kblcを、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵Ksesで暗号化させる。記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとブロック鍵Kblcを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デ

バイスコントローラ 303 を介して記録デバイス 400 に送信する。

次に、ステップ S165 において、記録再生器 300 から送信されてきたブロック情報鍵 K_{bit} とブロック鍵 K_{blc} を受信した記録デバイス 400 は、受信したデータを記録デバイス暗号処理部 401 の暗号／復号化部 406 に、相互認証の際に共有しておいたセッション鍵 K_{ses} で復号化させ、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵 K_{str} で再暗号化させ、記録再生器 300 の制御部 301 は、記録再生器 300 の記録デバイスコントローラ 303 を介し、記録デバイス 400 から保存鍵 K_{str} で再暗号化されたブロック情報鍵 K_{bit} とブロック鍵 K_{blc} を読み出す。すなわち、当初、配送鍵 K_{dis} で暗号化されたブロック情報鍵 K_{bit} とブロック鍵 K_{blc} を保存鍵 K_{str} で再暗号化されたブロック情報鍵 K_{bit} とブロック鍵 K_{blc} へ置き換えを行なう。

以下のステップ S119～S122 は、前述のフォーマットタイプ 0, 1, 2 と同様であるので説明を省略する。

以上が、フォーマットタイプ 3 におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ 3 のダウンロード処理は、フォーマットタイプ 2 と同様、ブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。また、ブロック鍵 K_{blc} により暗号化コンテンツを保護する範囲が局所化されているので、フォーマットタイプ 2 に比較して、よりセキュリティが高度となる。

次に、フォーマットタイプ 0～3 各々における記録再生器 300 における記録デバイス 400 からの再生処理について図 42～45 のフローを用いて説明する。

まず、フォーマットタイプ 0 におけるコンテンツの再生処理について図 42 を用いて説明する。

ステップ S201 は、記録再生器と記録デバイス間における認証処理ステップ

であり、先に説明した図20の認証処理フローに従って実行される。

ステップS201の認証処理が終了し、認証フラグがセットされると、記録再生器300は、ステップS202において、記録デバイス400から所定のフォーマットに従ったデータのヘッダを読み出し、記録再生器300の記録再生器暗号処理部302に送信する。

次に、ステップS203において、暗号処理部302の制御部306が記録再生器暗号処理部302の暗号／復号化部308にチェック値Aを計算させる。チェック値Aは、先に説明した図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵*K_{icva}*を鍵とし、識別情報（*Content ID*）と取扱方針（*Usage Policy*）をメッセージとして計算される。次に、ステップS204において、計算されたチェック値Aとヘッダ（*Header*）内に格納されたチェック値：*ICVa*を比較し、一致していた場合にはステップS205へ進む。

チェック値A、*ICVa*は、識別情報、取扱方針の改竄を検証するためのチェック値である。計算されたチェック値Aが、ヘッダ（*Header*）内に格納されたチェック値：*ICVa*と一致した場合には、記録デバイス400に格納された識別情報、取扱方針の改竄はないと判断される。

次に、ステップS205において、記録再生器300の制御部301は、読み出したヘッダから記録デバイス固有の保存鍵*K_{str}*で暗号化されたブロック情報鍵*K_{bit}*とコンテンツ鍵*K_{con}*を取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

記録再生器300から送信されてきたブロック情報鍵*K_{bit}*とコンテンツ鍵*K_{con}*を受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵*K_{str}*で復号化処理させ、相互認証の際に共有しておいたセッション鍵*K_{ses}*で再び暗号化させる。この処理は、前述した（9）相互認証後の鍵交換処理の欄で詳しく述べた通りで

ある。

ステップS206では、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを受信する。

次に、ステップS207において、記録再生器300の制御部301は、受信したセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを記録再生器300の記録再生器暗号処理部302に送信し、セッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の暗号／復号化部308に、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを、相互認証の際に共有しておいたセッション鍵Ksesで復号化させる。

さらに、ステップS208において、復号化したブロック情報鍵Kbitで、ステップS202で読み出しておいたブロック情報を復号化する。なお、記録再生器300の記録再生器暗号処理部302は、復号化したブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITを、ステップS202で読み出したヘッダに含まれるブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITに置き換えて保持しておく。また、記録再生器300の制御部301は、復号化されたブロック情報BITを記録再生器300の記録再生器暗号処理部302から読み出しておく。

さらに、ステップS209において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)から、チェック値B(ICVb')を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)からなる排他的論理和値をDES

で暗号化して生成する。次に、ステップS 2 1 0において、チェック値Bとヘッダ (H e a d e r) 内のI C V bを比較し、一致していた場合にはステップS 2 1 1へ進む。

チェック値B、I C V bは、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄を検証するためのチェック値であり、生成したチェック値Bが、ヘッダ (H e a d e r) 内に格納されたチェック値：I C V bと一致した場合には、記録デバイス4 0 0に保存されたデータ中のブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄はないと判断される。

ステップS 2 1 1において、記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8に中間チェック値の計算をさせる。中間チェック値は、図2 5に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されている総チェック値生成鍵K i c v tを鍵とし、検証したH e a d e r内のチェック値A、チェック値B、ブロック情報中の全てのコンテンツチェック値をメッセージとして図7他で説明したI C V計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器3 0 0の記録再生器暗号処理部3 0 2に保持しておく。

次に、ステップS 2 1 2において、記録再生器3 0 0の制御部3 0 1は、記録デバイス4 0 0の外部メモリ4 0 2から読み出したデータのヘッダ部に含まれる取扱方針 (U s a g e P o l i c y) から利用制限情報を取り出し、再生予定のコンテンツが当該記録再生器3 0 0のみで利用できる (利用制限情報が1) か、別の同様な記録再生器3 0 0でも利用できる (利用制限情報が0) か判定する。判定の結果、利用制限情報が1、すなわち再生コンテンツが当該記録再生器3 0 0のみで利用できる利用制限が設定されている場合には、ステップS 2 1 3に進み、利用制限情報が0、すなわち別の同様な記録再生器3 0 0でも利用できる設定であった場合には、ステップS 2 1 5に進む。なお、ステップS 2 1 2の処理は暗号処理部3 0 2が行なってもよい。

ステップS 2 1 3では、記録再生器3 0 0の制御部3 0 1は、記録再生器固有

のチェック値 ICV_{dev}' を記録再生器 300 の記録再生器暗号処理部 302 に計算させる。記録再生器固有のチェック値 ICV_{dev}' は、図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されている記録再生器署名鍵 K_{dev} を鍵とし、ステップ S 211 で保持しておいた中間チェック値を DES で暗号化して生成する。

次に、ステップ S 214 において、ステップ S 213 で計算した記録再生器固有のチェック値 ICV_{dev}' とステップ S 202 で読み出したヘッダ内の ICV_{dev} を比較し、一致していた場合には、ステップ S 217 へ進む。

一方ステップ S 215 では、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に総チェック値 ICV_t の計算をさせる。総チェック値 ICV_t' は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているシステム署名鍵 K_{sys} を鍵とし、中間チェック値を DES で暗号化して生成する。次に、ステップ S 216 において、生成した総チェック値 ICV_t' とヘッダ (Header) 内の ICV_t を比較し、一致していた場合には、ステップ S 217 へ進む。

総チェック値 ICV_t 、および記録再生器固有のチェック値 ICV_{dev} は、 ICV_a 、 ICV_b 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成されたチェック値がヘッダ (Header) 内に格納されたチェック値： ICV_t または ICV_{dev} と一致した場合には、記録デバイス 400 に格納された ICV_a 、 ICV_b 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

次に、ステップ S 217 において、記録再生器 300 の制御部 301 は、記録デバイス 400 からブロックデータを読み出す。さらに、ステップ S 218 において暗号化されているか否かを判定し、暗号化されている場合は、記録再生器 300 の暗号処理部 302 においてブロックデータの復号を行なう。暗号化されていない場合は、ステップ S 219 をスキップしてステップ S 220 へ進む。

次に、ステップ S 220 において、記録再生器 300 の制御部 301 は、プロ

ック情報 (B I T) 内のコンテンツブロック情報に基づいて、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。コンテンツブロックが検証対象になっていた場合には、ステップ S 2 2 1 において、該当するコンテンツブロックのコンテンツチェック値 ICV_i' を計算させる。コンテンツブロックが検証対象になっていない場合には、ステップ S 2 2 1 と S 2 2 2 をスキップしてステップ S 2 2 3 に進む。

コンテンツチェック値 ICV_i' は、先に図 3 6 で説明したようにブロックが暗号化されている場合、コンテンツ鍵 K_{con} で、入力されたコンテンツブロックを DES の CBC モードで復号化し、その結果を全て 8 バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器 3 0 0 の内部メモリ 3 0 7 に格納されたコンテンツチェック値生成鍵 K_{icvc} で暗号化して生成する。また、ブロックが暗号化されていない場合は、データ (平文) 全体を 8 バイト単位で図 3 6 に示す改竄チェック値生成関数 (DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする) に入力して得た値として生成される。

ステップ S 2 2 2 においては、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、生成したコンテンツチェック値 ICV_i' と、ステップ S 2 0 2 で記録デバイス 4 0 0 から受信したヘッダ部に格納されたコンテンツチェック値 ICV_i とを比較し、その結果を記録再生器 3 0 0 の制御部 3 0 1 に渡す。これを受信した記録再生器 3 0 0 の制御部 3 0 1 は、検証に成功していた場合、ステップ S 2 2 3 において、記録再生器システム RAM 上に実行 (再生) 用コンテンツ平文データを格納する。記録再生器 3 0 0 の制御部 3 0 1 は、さらに次の検証対象コンテンツブロックを取り出して記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理、RAM 格納処理を繰り返す (ステップ S 2 2 4)。

なお、ステップ S 2 0 4、ステップ S 2 1 0、ステップ S 2 1 4、ステップ S 2 1 6、ステップ S 2 2 2 のいずれかにおいて、チェック値の一致が得られなか

った場合はエラーとして再生処理は終了する。

ステップS 2 2 4において全ブロック読み出しと判定されると、ステップS 2 2 5に進み、コンテンツ（プログラム、データ）の実行、再生が開始される。

以上が、フォーマットタイプ0におけるコンテンツデータの再生処理の態様である。

次に、フォーマットタイプ1におけるコンテンツデータの再生処理について図4 3を用いて説明する。上記したフォーマットタイプ0の再生処理と異なる点を中心に説明する。

ステップS 2 0 1～ステップS 2 1 7までの処理は、上記したフォーマットタイプ0の再生処理と同様であるので説明は省略する。

フォーマットタイプ1では、ステップS 2 3 1において、暗号化パーツの復号が実行され、パーツICVが生成される。さらに、ステップS 2 3 2において、ブロックICV i が生成される。先に説明したように、フォーマット・タイプ1においては、ブロック内のパーツのうち少なくとも1つがチェック値ICV i の対象データである場合は、そのブロックに関してコンテンツチェック値ICV i が定義される。ブロック i におけるパーツ j のチェック値P-ICV ij は、パーツ j が暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値をコンテンツチェック値生成鍵 K_{icvc} で暗号化した値として生成される。また、パーツ j が暗号化されていない場合は、データ（平文）全体を8バイト単位で図3 6に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。

さらに、1つのブロック i 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが1つのみ存在する場合は、上述の手法で生成したチェック値P-ICV ij をそのままブロックのチェック値ICV i とし、また、1つのブロック i 内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが複数存在する場合

は、複数のパーツチェック値 $P - I C V i, j$ をパーツ番号順に連結したデータを対象にしてデータ（平文）全体を 8 バイト単位で図 3 6 に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。これは、先に図 3 7 で説明した通りである。

フォーマットタイプ 1 では、上述の手順で生成されたコンテンツチェック値の比較処理がステップ S 2 2 2 で実行されることになる。以下のステップ S 2 2 3 以下の処理はフォーマットタイプ 0 と同様であるので説明は省略する。

次に、フォーマットタイプ 2 におけるコンテンツデータの再生処理について図 4 4 を用いて説明する。上記したフォーマットタイプ 0, 1 の再生処理と異なる点を中心に説明する。

ステップ S 2 0 1 ~ S 2 1 0 は、上記したフォーマットタイプ 0, 1 の再生処理と同様であるので説明は省略する。

フォーマットタイプ 2 においては、フォーマットタイプ 0, 1 において実行されたステップ S 2 1 1 ~ S 2 1 6 の処理が実行されない。また、フォーマットタイプ 2 においては、コンテンツチェック値を持たないため、フォーマットタイプ 0, 1 において実行されたステップ S 2 2 2 のコンテンツチェック値の検証も実行されない。

フォーマットタイプ 2 のデータ再生処理においては、ステップ S 2 1 0 のチェック値 B の検証ステップの後、ステップ S 2 1 7 に進み、記録再生器 3 0 0 の制御部 3 0 1 の制御によって、ブロックデータが読み出される。さらに、ステップ S 2 4 1 において、記録再生器 3 0 0 の暗号処理部 3 0 6 によるブロックデータに含まれるブロック鍵 K_{b1c} の復号処理が実行される。記録デバイス 4 0 0 に格納されたブロック鍵 K_{b1c} は、図 3 4 で示すようにコンテンツ鍵 K_{con} で暗号化されており、先のステップ S 2 0 7 において復号したコンテンツ鍵 K_{con} を用いてブロック鍵 K_{b1c} の復号を行なう。

次に、ステップ S 2 4 2 において、ステップ S 2 4 1 で復号されたブロック鍵

K b l c を用いてブロックデータの復号処理が実行される。さらに、ステップ S 2 4 3 において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップ S 2 1 7 ～ステップ S 2 4 3 の処理が全ブロックについて繰り返し実行される。ステップ S 2 4 4 において全ブロック読み出しと判定されると再生処理は終了する。

このようにフォーマットタイプ 2 の処理は、総チェック値等のチェック値検証処理を省略しており、高速な復号処理の実行に適している構成であり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

次にフォーマットタイプ 3 におけるコンテンツデータの再生処理について図 4 5 を用いて説明する。上記したフォーマットタイプ 0, 1, 2 の再生処理と異なる点を中心に説明する。

フォーマットタイプ 3 は、基本的にフォーマットタイプ 2 における処理と共通する部分が多いが、フォーマットタイプ 3 は図 3 5 において説明したようにコンテンツ鍵を有しておらず、またブロック鍵 K b l c が記録デバイスにおいては保存鍵 K s t r で暗号化されて格納される点がフォーマットタイプ 2 と異なる。

ステップ S 2 0 1 ～ S 2 1 0 において、ステップ S 2 5 1、ステップ S 2 5 2、ステップ S 2 5 3、ステップ S 2 5 4 の処理は、前述のフォーマットタイプ 0, 1, 2 における対応処理と異なりコンテンツ鍵を含まない処理として構成されている。

ステップ S 2 5 1 において、記録再生器 3 0 0 の制御部 3 0 1 は、読み出したヘッダから記録デバイス固有の保存鍵 K s t r で暗号化されたブロック情報鍵 K b i t を取り出し、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介して記録デバイス 4 0 0 に送信する。

記録再生器 3 0 0 から送信されてきたブロック情報鍵 K b i t を受信した記録デバイス 4 0 0 は、受信したデータを記録デバイス暗号処理部 4 0 1 の暗号／復号化部 4 0 6 に、記録デバイス暗号処理部 4 0 1 の内部メモリ 4 0 5 に保存してある記録デバイス固有の保存鍵 K s t r で復号化処理させ、相互認証の際に共有

しておいたセッション鍵K s e sで再暗号化させる。この処理は、前述した（9）相互認証後の鍵交換処理の欄で詳しく述べた通りである。

ステップS 2 5 2では、記録再生器3 0 0の制御部3 0 1は、記録再生器3 0 0の記録デバイスコントローラ3 0 3を介し、記録デバイス4 0 0からセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tを受信する。

次に、ステップS 2 5 3において、記録再生器3 0 0の制御部3 0 1は、受信したセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tを記録再生器3 0 0の記録再生器暗号処理部3 0 2に送信し、セッション鍵K s e sで再暗号化されたブロック情報鍵K b i tを受信した記録再生器3 0 0の記録再生器暗号処理部3 0 2は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8に、セッション鍵K s e sで暗号化されたブロック情報鍵K b i tを、相互認証の際に共有しておいたセッション鍵K s e sで復号化させる。

さらに、ステップS 2 0 8において、復号化したブロック情報鍵K b i tで、ステップS 2 0 2で読み出しておいたブロック情報を復号化する。なお、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、復号化したブロック情報鍵K b i tおよびブロック情報B I Tを、ステップS 2 0 2で読み出したヘッダに含まれるブロック情報鍵K b i tおよびブロック情報B I Tに置き換えて保持しておく。また、記録再生器3 0 0の制御部3 0 1は、復号化されたブロック情報B I Tを記録再生器3 0 0の記録再生器暗号処理部3 0 2から読み出しておく。

さらに、ステップS 2 5 4において、記録再生器暗号処理部3 0 2の制御部3 0 6は、ブロック情報鍵K b i tおよびブロック情報（B I T）から、チェック値B（I C V b'）を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値B生成鍵K i c v bを鍵とし、ブロック情報鍵K b i tおよびブロック情報（B I T）からなる排他的論理和値をD E Sで暗号化して生成する。次に、ステップS 2 1 0において、チェック値Bとヘッダ（H e a d e r）内のI C V bを比較し、一致していた場合にはステップS 2 1 1へ進む。

フォーマットタイプ3では、さらに、ブロック鍵が記録デバイスでの格納時に保存鍵によって暗号化されるため、記録デバイス400における保存鍵での復号処理、およびセッション鍵での暗号化処理、さらに、記録再生器300でのセッション鍵での復号処理が必要となる。これらの一連の処理がステップS255、ステップS256で示した処理ステップである。

ステップS255では、記録再生器300の制御部301は、ステップS217で読み出したブロックから記録デバイス固有の保存鍵K_{str}で暗号化されたブロック鍵K_{blc}を取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

記録再生器300から送信されてきたブロック鍵K_{blc}を受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K_{str}で復号化処理させ、相互認証の際に共有しておいたセッション鍵K_{ses}で再暗号化させる。この処理は、前述した「(9) 相互認証後の鍵交換処理」の欄で詳しく述べた通りである。

ステップS256では、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵K_{ses}で再暗号化されたブロック鍵K_{blc}を受信する。

次に、ステップS257において、記録再生器300の暗号処理部306によるブロック鍵K_{blc}のセッション鍵K_{ses}を用いた復号処理が実行される。

次に、ステップS242において、ステップS257で復号されたブロック鍵K_{blc}を用いてブロックデータの復号処理が実行される。さらに、ステップS243において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップS217～ステップS243の処理が全ブロックについて繰り返して実行される。ステップS244において全ブロック読み出しと判定されると再生処理は終了する。

以上の処理が、フォーマットタイプ3におけるコンテンツの再生処理である。

総チェック値の検証処理が省略された点でフォーマットタイプ2と類似するが、ブロック鍵の鍵交換処理を含む点でフォーマットタイプ2に比較して、さらにセキュリティ・レベルの高い処理構成となっている。

(11) コンテンツプロバイダにおけるチェック値 (ICV) 生成処理態様

上述の実施例中において、各種のチェック値 ICV についての検証処理が、コンテンツのダウンロード、または再生処理等の段階で実行されることを説明してきた。ここでは、これら各チェック値 (ICV) 生成処理、検証処理の態様について説明する。

まず、実施例で説明した各チェック値について、簡潔にまとめると、本発明のデータ処理装置において利用されるチェック値 ICV には以下のものがある。

チェック値 A, ICV a : コンテンツデータ中の識別情報、取扱方針の改竄を検証するためのチェック値。

チェック値 B, ICV b : ブロック情報鍵 K b i t、コンテンツ鍵 K c o n、ブロック情報の改竄を検証するためのチェック値。

コンテンツチェック値 ICV i : コンテンツの各コンテンツブロックの改竄を検証するためのチェック値。

総チェック値 ICV t : チェック値 ICV a、チェック値 ICV b、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。

再生器固有チェック値 ICV d e v : ローカリゼーションフラグが1にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 ICV t に置き換えられるチェック値であり、前述のチェック値 A : ICV a、チェック値 B : ICV b、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 ICV i 全体に対するチェック値として生成される。

フォーマットによっては、ICV t、ICV d e v がチェックする対象に含まれるのは、各コンテンツブロックのチェック値ではなく、コンテンツそのものとなる場合もある。

以上の各チェック値が本発明のデータ処理装置において用いられる。上記各チェック値の中で、チェック値A、チェック値B、総チェック値、コンテンツチェック値は、例えば図32～35、および図6に示されるようにコンテンツデータを提供するコンテンツプロバイダ、あるいはコンテンツ管理者によって、それぞれの検証対象データに基づいてICV値が生成され、コンテンツと共にデータ中に格納されて記録再生器300の利用者に提供される。記録再生器の利用者、すなわちコンテンツ利用者は、このコンテンツを記録デバイスにダウンロードする際、または再生する際にそれぞれの検証対象データに基づいて検証用のICVを生成して、格納済みのICVとの比較を行なう。また、再生器固有チェック値ICVdevは、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値ICVtに置き換えられて、記録デバイスに格納されるものである。

チェック値の生成処理は、前述の実施例中では、主としてDES-CBCによる生成処理構成を説明してきた。しかし、ICVの生成処理態様には、上述の方法に限らず様々な生成処理態様、さらに、様々な検証処理態様がある。特にコンテンツ提供者または管理者と、コンテンツ利用者との関係においては、以下に説明する各種のICV生成および検証処理構成が可能である。

図46～図48にチェック値ICVの生成者における生成処理と、検証者による検証処理を説明する図を示す。

図46は、上述の実施例中で説明したDES-CBCによるICVの生成処理を、例えばコンテンツ提供者または管理者であるICV生成者が行ない、生成したICVをコンテンツと共に記録再生器利用者、すなわち検証者に提供する構成である。この場合に記録再生器利用者、すなわち検証者が検証処理の際に必要な鍵は、例えば図18に示す内部メモリ307に格納された各チェック値生成鍵である。コンテンツ利用者である検証者（記録再生器利用者）は、内部メモリ307に格納されたチェック値生成鍵を使用して、検証対象のデータにDES-CBCを適用してチェック値を生成して格納チェック値と比較処理を実行する。

この場合、各チェック値生成鍵は、ICVの生成者と、検証者が秘密に共有する鍵として構成される。

図47は、コンテンツ提供者または管理者であるICVの生成者が公開鍵暗号系のデジタル署名によりICVを生成して、生成したICVをコンテンツと共にコンテンツ利用者、すなわち検証者に提供する。コンテンツ利用者、すなわち検証者は、ICV生成者の公開鍵を保存し、この公開鍵を用いてICVの検証処理を実行する構成である。この場合、コンテンツ利用者（記録再生器利用者）、すなわち検証者の有するICV生成者の公開鍵は秘密にする必要がなく、管理は容易となる。ICVの生成、管理が1つのエンティティにおいて実行される場合等、ICVの生成、管理が高いセキュリティ管理レベルで行われている場合に適した態様である。

図48は、コンテンツ提供者または管理者であるICVの生成者が公開鍵暗号系のデジタル署名によりICVを生成して、生成したICVをコンテンツと共にコンテンツ利用者、すなわち検証者に提供し、さらに、検証者が検証に用いる公開鍵を公開鍵証明書（例えば図14参照）に格納してコンテンツデータと共に記録再生器利用者、すなわち検証者に提供する。ICVの生成者が複数存在する場合には、各生成者は、公開鍵の正当性を証明するデータ（公開鍵証明書）を鍵管理センタに作成してもらう。

ICVの検証者であるコンテンツ利用者は、鍵管理センタの公開鍵を持ち、検証者は公開鍵証明書の検証を鍵管理センタの公開鍵によって実行し、正当性が確認されたら、その公開鍵証明書に格納されたICVの生成者の公開鍵を取り出す。さらに、取り出したICVの生成者の公開鍵を用いてICVの検証を実行する。

この方法は、ICVの生成者が複数あり、それらの管理を実行するセンタによる管理の実行システムが確立している場合に有効な態様である。

(1.2) マスタ鍵に基づく暗号処理鍵生成構成

次に、本発明のデータ処理システムにおける特徴的な構成の1つである、マス

タ鍵に基づく各種暗号処理用鍵の生成構成について説明する。

先に図18を用いて説明したように、本発明のデータ処理装置における記録再生器300の内部メモリには、様々なマスタ鍵が格納され、これらの各マスタ鍵を用いて、例えば認証鍵Kakeを生成（数3参照）したり、あるいは配送鍵Kdisを生成（数4参照）する構成となっている。

従来、1対1のエンティティ間、すなわちコンテンツプロバイダとコンテンツ利用者間、あるいは、上述の本発明のデータ処理装置における記録再生器300と記録メディア400との間において暗号通信、相互認証、MAC生成、検証等を行なう際には、各エンティティに共通な秘密情報、例えば鍵情報を保持させていた。また、1対多の関係、例えば1つのコンテンツプロバイダに対する多数のコンテンツ利用者、あるいは1つの記録再生器に対する多数の記録メディア等の関係においては、すべてのエンティティ、すなわち多数のコンテンツ利用者、あるいは多数の記録メディアにおいて共有させた秘密情報、例えば鍵情報を格納保持させる構成とするか、あるいは、1つのコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報（ex. 鍵）を個別に管理し、これを各コンテンツ利用者に応じて使い分けていた。

しかしながら、上記のような1対多の利用関係がある場合、すべてが共有する秘密情報（ex. 鍵）を所有する構成においては、1箇所の秘密漏洩が発生すると同じ秘密情報（ex. 鍵）を利用している者すべてに影響が及ぶという欠点がある。また、1つの管理者、例えばコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報（ex. 鍵）を個別に管理し、これを各コンテンツ利用者に応じて使い分ける構成とすると、すべての利用者を識別し、かつその識別データに固有の秘密情報（ex. 鍵）を対応づけたリストが必要となり、利用者の増大に伴うリストの保守管理の負担が増加するという欠点がある。

本発明のデータ処理装置においては、このようなエンティティ間における秘密情報の共有における従来の問題点をマスター鍵の保有、およびマスター鍵から各種の個別鍵を生成する構成により解決した。以下、この構成について説明する。

本発明のデータ処理装置においては、記録デバイスやコンテンツを格納したメディア、または記録再生器間での各種の暗号処理、認証処理等において異なる個別の鍵が必要になる場合、その個別の鍵を、デバイスやメディアが固有に持つ識別子データ（ID）などの個別情報と記録再生器300内であらかじめ決められた個別鍵生成方式を用いて生成する。この構成により万が一、生成された個別の鍵が特定された場合でもマスター鍵の漏洩を防止すれば、システム全体への被害を防ぐことが可能となる。またマスター鍵によって鍵を生成する構成により対応づけリストの管理も不要となる。

具体的な構成例について、図を用いて説明する。まず、図49に各種の鍵を記録再生器300の有する各種のマスタ鍵を用いて生成する構成を説明する図を示す。図49のメディア500、通信手段600からは、すでに説明した実施例と同様、コンテンツが入力される。コンテンツはコンテンツ鍵Kconによって暗号化され、またコンテンツ鍵Kconは、配送鍵Kdisによって暗号化されている。

例えば、記録再生器300がメディア500、通信手段600からコンテンツを取り出して、記録デバイス400にダウンロードしようとする場合、先の図22、図39～41において説明したように、記録再生器300は、コンテンツ鍵を暗号化している配送鍵Kdisを取得することが必要となる。このKdisをメディア500、通信手段600から直接取得したり、あるいは予め記録再生器300が取得して記録再生器300内のメモリに格納しておくことも可能であるが、このような鍵の多数のユーザに対する配布構成は、先にも説明したようにシステム全体に影響を及ぼす漏洩の可能性がある。

本発明のデータ処理システムでは、この配送鍵Kdisを図49の下部に示すように、記録再生器300のメモリに格納された配送鍵用マスター鍵MKdisと、コンテンツIDに基づく処理、すなわち $Kdis = DES(MKdis, \text{コンテンツID})$ を適用して配送鍵Kdisを生成する構成としている。本構成によれば、メディア500、通信手段600からコンテンツを供給するコンテンツ

プロバイダとそのコンテンツ利用者である記録再生器 300 間におけるコンテンツ配布構成において、コンテンツプロバイダが多数存在した場合であっても、個々の配送鍵 K_{dis} をメディア、通信媒体等を介して流通させる必要もなく、また、各記録再生器 300 に格納する必要もなく、セキュリティを高度に保つことが可能となる。

次に、認証鍵 K_{ake} の生成について説明する。先に説明した図 22、図 39～41 の記録再生器 300 から記録メディア 400 に対するダウンロード処理、あるいは図 28、図 42～45 で説明した記録メディア 400 に格納されたコンテンツを記録再生器 300 において実行、再生する場合、記録再生器 300 と記録メディア 400 間における相互認証処理（図 20 参照）が必要となる。

図 20 で説明したように、この認証処理において記録再生器 300 は認証鍵 K_{ake} が必要となる。記録再生器 300 は、認証鍵を例えば記録メディア 400 から直接取得したり、あるいは予め記録再生器 300 が取得して記録再生器 300 内のメモリに格納しておくことも可能であるが、上述の配送鍵の構成と同様、このような鍵の多数のユーザに対する配布構成は、システム全体に影響を及ぼす漏洩の可能性がある。

本発明のデータ処理システムでは、この認証鍵 K_{ake} を図 49 の下部に示すように、記録再生器 300 のメモリに格納された認証鍵用マスター鍵 MK_{ake} と、記録デバイス識別 ID: ID_{mem} に基づく処理、すなわち $K_{ake} = DES(MK_{ake}, ID_{mem})$ によって認証鍵 K_{ake} を求める構成としている。

さらに、図 22、図 39～41 の記録再生器 300 から記録メディア 400 に対するダウンロード処理、あるいは図 28、図 42～45 で説明した記録メディア 400 に格納されたコンテンツを記録再生器 300 において実行、再生する場合、記録再生器固有に利用可能なコンテンツである場合の記録再生器固有チェック値 ICV_{dev} の生成処理に必要な記録再生器署名鍵 K_{dev} についても上述の配送鍵、認証鍵と同様の構成とすることができる。上述の実施例中では、

記録再生器署名鍵 K_{dev} は内部メモリに格納する構成としていたが、記録再生器署名鍵用マスター鍵 MK_{dev} をメモリに格納し、記録再生器署名鍵 K_{dev} は内部メモリに格納せず、必要に応じて図 49 の下部に示すように記録再生器識別子: ID_{dev} と記録再生器署名鍵用マスター鍵 MK_{dev} に基づいて、 $K_{dev} = DES(MK_{dev}, ID_{dev})$ によって記録再生器署名鍵 K_{dev} を求める構成とすることで、記録再生器署名鍵 K_{dev} を機器個別に持たせる必要がなくなるという利点が挙げられる。

このように、本発明のデータ処理装置においては、プロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような 2 つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各 ID から逐次的に生成する構成としたので、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。

本構成に関する複数の処理例についてフローを示して説明する。図 50 は、コンテンツ製作または管理者におけるマスター鍵を用いたコンテンツ等の暗号化処理と、ユーザデバイス、例えば上述の実施例における記録再生器 300 におけるマスター鍵を用いた暗号化データの復号処理例である。

コンテンツ製作または管理者におけるステップ S501 は、コンテンツに対する識別子 (コンテンツ ID) を付与するステップである。ステップ S502 は、コンテンツ製作または管理者の有するマスター鍵とコンテンツ ID とに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵 K_{dis} を生成する工程とすれば、前述の $K_{dis} = DES(MK_{dis}, \text{コンテンツ } ID)$ によって配送鍵 K_{dis} を生成する。次に、ステップ S503 は、コンテンツの一部、または全部を鍵 (例えば配送鍵 K_{dis}) によって暗号化するステップである。コンテンツ製作者は、このようなステップを経て暗号化処理を行なったコンテンツを DVD 等のメディア、通信手段等を介して配信する。

一方、例えば記録再生器 300 等のユーザデバイス側では、ステップ S504

において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツIDを読み出す。次に、ステップS505において、読み出したコンテンツIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 K_{dis} を得るものである場合は、例えば配送鍵 $K_{dis} = DES(MK_{dis}, \text{コンテンツID})$ となる。ステップS506で、この鍵を用いてコンテンツを復号し、ステップS507で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

この例においては、図50下段に示すように、コンテンツ製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵 MK_{dis} ）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ID（コンテンツID）に基づいて生成する。

このシステムでは、万が一配送鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、コンテンツIDの異なる他のコンテンツの復号は防止することが可能であるため、1つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

次に図51を用いて、コンテンツ製作または管理者が複数のマスター鍵を所有して、コンテンツの配信対象に応じた処理を実行する例について説明する。

コンテンツ製作または管理者におけるステップS511は、コンテンツに対する識別子（コンテンツID）を付与するステップである。ステップS512は、コンテンツ製作または管理者の有する複数のマスター鍵（例えば複数の配送鍵生成用マスター鍵 MK_{dis} ）から1つのマスター鍵を選択するステップである。この選択処理は図52を用いてさらに説明するが、コンテンツの利用者の国ごと、機種ごと、あるいは機種のバージョンごとなどに対応付けて予め適用するマスター鍵を設定しておき、その設定に従って実行するものである。

次に、ステップS513では、ステップS512で選択したマスター鍵と、ス

ステップS 5 1 1 で決定したコンテンツIDとに基づいて暗号化用の鍵を生成する。これは例えば、配送鍵 K_{disi} を生成する工程とすれば、 $K_{disi} = DES(MK_{disi}, \text{コンテンツID})$ によって生成する。次に、ステップS 5 1 4 はコンテンツの一部、または全部を鍵（例えば配送鍵 K_{disi} ）によって暗号化するステップである。コンテンツ製作者は、ステップS 5 1 5 において、コンテンツIDと、使用したマスター鍵識別情報と、暗号化コンテンツを1つの配布単位として暗号化処理を行なったコンテンツをDVD等のメディア、通信手段等を介して配信する。

一方、例えば記録再生器300等のユーザデバイス側では、ステップS 5 1 6 において、DVD等のメディア、通信手段等を介して配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有するか否かについて判定する。コンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を持たない場合は、その配布コンテンツは、そのユーザデバイスにおいては利用できないものであり、処理は終了する。

配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有する場合は、ステップS 5 1 7 において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツIDを読み出す。次に、ステップS 5 1 8 において、読み出したコンテンツIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 K_{disi} を得るものである場合は、例えば配送鍵 $K_{disi} = DES(MK_{disi}, \text{コンテンツID})$ となる。ステップS 5 1 9 で、この鍵を用いてコンテンツを復号し、ステップS 5 2 0 で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

この例においては、図51下段に示すように、コンテンツ製作または管理者は、複数のマスター鍵、例えば複数の配送鍵生成用マスター鍵 $MK_{dis1} \sim n$ からなるマスター鍵セットを有する。一方、ユーザデバイスには1つのマスター鍵例えば1つの配送鍵生成用マスター鍵 KK_{disi} を有し、コンテンツ製作また

は管理者がMK d i s i を用いて暗号化処理している場合のみ、ユーザデバイスは、そのコンテンツを復号して利用することができる。

この図51のフローに示す態様の具体例として、国毎に異なるマスター鍵を適用した例を図52に示す。コンテンツプロバイダは、マスター鍵MK1～nを有し、MK1は日本向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いる。例えば、コンテンツIDとMK1から暗号化鍵K1を生成してK1によってコンテンツを暗号化する。また、MK2はUS向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用い、MK3はEU（ヨーロッパ）向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いるよう設定している。

一方、日本向けユーザデバイス、具体的には日本で販売されるPCまたはゲーム機器等の記録再生器には、マスター鍵MK1がその内部メモリに格納され、US向けユーザデバイスには、マスター鍵MK2がその内部メモリに格納され、EU向けユーザデバイスには、マスター鍵MK3がその内部メモリに格納されている。

このような構成において、コンテンツプロバイダは、コンテンツを利用可能なユーザデバイスに応じて、マスター鍵MK1～nから、マスター鍵を選択的に使用してユーザデバイスに配信するコンテンツの暗号化処理を実行する。例えばコンテンツを日本向けのユーザデバイスのみ利用可能とするためには、マスター鍵MK1を用いて生成された鍵K1によってコンテンツを暗号化する。この暗号化コンテンツは、日本向けユーザデバイスに格納されたマスター鍵MK1を用いて復号可能、すなわち復号鍵を生成可能であるが、他のUS、またはEU向けのユーザデバイスに格納されたマスター鍵MK2、MK3からは鍵K1を得ることができないので、暗号化コンテンツの復号は不可能となる。

このように、コンテンツプロバイダが複数のマスター鍵を選択的に使用することにより、様々なコンテンツの利用制限を設定することができる。図52では、ユーザデバイスの国別にマスター鍵を区別する例を示したが、前述のように、ユ

ーザデバイスの機種に応じて、あるいはバージョンに応じてマスター鍵を切り換える等、様々な利用形態が可能である。

次に、図53にメディア固有の識別子、すなわちメディアIDとマスター鍵を組み合わせた処理例を示す。ここで、メディアとは例えばDVD、CD等のコンテンツを格納したメディアである。メディアIDは、1つ1つのメディアごとに固有としてもよいし、たとえば、映画などのコンテンツのタイトルごとに固有としてもよいし、メディアの製造ロットごとに固有としてもよい。このようにメディアIDの割り当て方法としては様々な方法を用いることができる。

メディア製作または管理者におけるステップS521は、メディアに対する識別子（メディアID）を決定するステップである。ステップS522は、メディア製作または管理者の有するマスター鍵とメディアIDとに基づいてメディア内の格納コンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵 K_{dis} を生成する工程とすれば、前述の $K_{dis} = DES(MK_{dis}, \text{メディアID})$ によって配送鍵 K_{dis} を生成する。次に、ステップS523は、メディア格納コンテンツの一部、または全部を鍵（例えば配送鍵 K_{dis} ）によって暗号化するステップである。メディア製作者は、このようなステップを経て暗号化処理を行なったコンテンツ格納メディアを供給する。

一方、例えば記録再生器300等のユーザデバイス側では、ステップS524において、供給されたメディアからメディアIDを読み出す。次に、ステップS525において、読み出したメディアIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 K_{dis} を得るものである場合は、例えば配送鍵 $K_{dis} = DES(MK_{dis}, \text{メディアID})$ となる。ステップS526で、この鍵を用いてコンテンツを復号し、ステップS527で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

この例においては、図53下段に示すように、メディア製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵 MK_{dis}

)を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ID(メディアID)に基づいて生成する。

このシステムでは、万が一メディア鍵が第三者に漏洩した場合、そのメディア内のコンテンツの復号が第三者において可能となるが、メディアIDの異なる他のメディアに格納されたコンテンツの復号は防止することが可能であるため、1つのメディア鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、メディア毎の鍵の対応付けリストを保持する必要がないという効果もある。また、1つのメディア鍵で暗号化されるコンテンツサイズは、そのメディア内に格納可能な容量に制限されるため、暗号文攻撃のために必要な情報量に達する可能性は少なく、暗号解読の可能性を低減させることができる。

次に、図54に記録再生器固有の識別子、すなわち記録再生器IDとマスター鍵を組み合わせた処理例を示す。

記録再生器利用者におけるステップS531は、記録再生器の例えば内部メモリに格納されたマスター鍵と記録再生器IDとに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、コンテンツ鍵 K_{con} を生成する工程とすれば、 $K_{con} = DES(MK_{con}, \text{記録再生器ID})$ によってコンテンツ鍵 K_{con} を生成する。次に、ステップS532は、格納するコンテンツの一部、または全部を鍵(例えば配送鍵 K_{con})によって暗号化するステップである。ステップS533は、暗号化コンテンツを例えばハードディスク等の記録デバイスに格納する。

一方、記録再生器を管理するシステム管理者側では、コンテンツを格納した記録再生器利用者から格納データの復旧を依頼されると、ステップS534において、記録再生器から、記録再生器IDを読み出す。次に、ステップS535において、読み出した記録再生器IDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、コンテンツ鍵 K_{con} を得るものである場合は、例えばコンテンツ鍵 $K_{con} = DES(MK_{con}, \text{記$

録再生器 I D) となる。ステップ S 5 3 6 で、この鍵を用いてコンテンツを復号する。

この例においては、図 5 4 下段に示すように、記録再生器利用者と、システム管理者の双方がマスター鍵（例えばコンテンツ鍵生成用マスター鍵 M K c o n）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各 I D（記録再生器 I D）に基づいて生成する。

このシステムでは、万が一コンテンツ鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、記録再生器 I D の異なる他の記録再生器用に暗号化されたコンテンツの復号は防止することが可能であるため、1つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、システム管理側、ユーザデバイス側両者において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

図 5 5 は、スレーブデバイス、例えばメモリカード等の記録デバイスと、ホストデバイス、例えば記録再生器間における相互認証処理に用いる認証鍵をマスター鍵に基づいて生成する構成である。先に説明した認証処理（図 2 0 参照）では、スレーブデバイスの内部メモリに認証鍵を予め格納した構成としてあるが、これを図 5 5 に示すように認証処理時にマスター鍵に基づいて生成する構成とすることができる。

例えば記録デバイスであるスレーブデバイスは、認証処理開始前の初期化处理として、ステップ S 5 4 1 において、記録デバイスであるスレーブデバイスの内部メモリに格納したマスター鍵とスレーブデバイス I D とに基づいて相互認証処理に用いる認証鍵 K a k e を生成する。これは例えば、 $K a k e = DES (MK a k e, \text{スレーブデバイス I D})$ によって生成する。次に、ステップ S 5 4 2 において、生成した認証鍵をメモリに格納する。

一方、例えば記録再生器等のホストデバイス側では、ステップ S 5 4 3 において、装着された記録デバイス、すなわちスレーブデバイスから、通信手段を介してスレーブデバイス I D を読み出す。次に、ステップ S 5 4 4 において、読み出

したスレーブデバイスIDと所有する認証鍵生成用マスター鍵に基づいて相互認証処理に適用する認証鍵を生成する。この生成処理は、例えば認証鍵 $K_{ake} = DES(MK_{ake}, \text{スレーブデバイスID})$ となる。ステップS545で、この認証鍵を用いて認証処理を実行する。

この例においては、図55下段に示すように、スレーブデバイスと、マスターデバイスの双方がマスター鍵、すなわち認証鍵生成用マスター鍵 MK_{ake} を有し、相互認証処理に必要な認証鍵を逐次的にそれぞれの所有するマスター鍵とスレーブデバイスIDに基づいて生成する。

このシステムでは、万が一認証鍵が第三者に漏洩した場合、その認証鍵は、そのスレーブデバイスのみ有効であるため、他のスレーブデバイスとの関係においては、認証が成立しないことになり、鍵の漏洩によって発生する影響を最小限にすることができるという効果がある。

このように、本発明のデータ処理装置においては、コンテンツプロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような2つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各IDから逐次的に生成する構成とした。従って、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。

(13) 暗号処理における暗号強度の制御

上述した実施例において、記録再生器300と記録デバイス400間での暗号処理は、説明を理解しやすくするため、主として、先に図7を用いて説明したシングルDES構成による暗号処理を用いた例について説明してきた。しかしながら、本発明のデータ処理装置において適用される暗号化処理方式は上述したシングルDES方式に何ら限定されるものではなく、必要なセキュリティ状態に応じた暗号化方式を採用することが可能である。

例えば先に説明した図8～図10の構成のようなトリプルDES方式を適用してもよい。例えば図3に示す記録再生器300の暗号処理部302と、記録デバ

イス400の暗号処理部401の双方において、トリプルDES方式を実行可能な構成とし、図8～図10で説明したトリプルDES方式による暗号処理に対応する処理を実行する構成が可能である。

しかしながら、コンテンツの提供者は、コンテンツに応じて処理速度を優先してコンテンツ鍵KconをシングルDES方式による64ビット鍵構成とする場合もあり、また、セキュリティを優先してコンテンツ鍵KconをトリプルDES方式による128ビット、または192ビット鍵構成とする場合もある。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の構成をトリプルDES方式、シングルDES方式いずれか一方の方式のみに対応可能な構成とすることは好ましくない。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401は、シングルDES、トリプルDESいずれの方式にも対応可能とする構成が望ましい。

しかしながら、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の暗号処理構成をシングルDES方式、トリプルDES方式の双方を実行可能な構成とするためには、それぞれの別の回路、ロジックを構成しなければならない。例えば、記録デバイス400においてトリプルDESに対応する処理を実行するためには、先の図29に示すコマンドレジスタにトリプルDESの命令セットを新たに格納することが必要となる。これは記録デバイス400に構成する処理部の複雑化を招くこととなる。

そこで、本発明のデータ処理装置は、記録デバイス400側の暗号処理部401の有するロジックをシングルDES構成として、かつトリプルDES暗号化処理に対応した処理が実行可能で、トリプルDES方式による暗号化データ(鍵、コンテンツ等)を記録デバイスの外部メモリ402に格納することを可能とした構成を提案する。

例えば図32に示すデータフォーマットタイプ0の例において、記録再生器300から記録デバイス400に対してコンテンツデータのダウンロードを実行する際、先に説明したフォーマットタイプ0のダウンロードのフローを示す図39

のステップS 1 0 1で認証処理を実行し、ここでセッション鍵K s e sを生成する。さらに、ステップS 1 1 7において、記録再生器3 0 0側の暗号処理部3 0 2においてセッション鍵K s e sによるコンテンツ鍵K c o nの暗号化処理が実行され、この暗号化鍵が記録デバイス4 0 0に通信手段を介して転送され、ステップS 1 1 8において、この暗号化鍵を受信した記録デバイス4 0 0の暗号処理部4 0 3がセッション鍵K s e sによるコンテンツ鍵K c o nの復号処理を実行し、さらに、保存鍵K s t rによるコンテンツ鍵K c o nの暗号化処理を実行して、これを記録再生器3 0 0の暗号処理部3 0 2に送信し、その後、記録再生器3 0 0がデータフォーマットを形成（ステップS 1 2 1）してフォーマット化されたデータを記録デバイス4 0 0に送信し、記録デバイス4 0 0が受信したデータを外部メモリ4 0 2に格納する処理を行なっている。

上記処理においてステップS 1 1 7， S 1 1 8間において実行される記録デバイス4 0 0の暗号処理部4 0 1での暗号処理をシングルDES、またはトリプルDESいずれかの方式を選択的に実行可能な構成とすれば、コンテンツ提供業者がトリプルDESにしたがったコンテンツ鍵K c o nを用いたコンテンツデータを提供する場合も、またシングルDESにしたがったコンテンツ鍵K c o nを用いたコンテンツデータを提供する場合も、いずれの場合にも対応可能となる。

図5 6に本発明のデータ処理装置における記録再生器3 0 0の暗号処理部3 0 2と、記録デバイス4 0 0の暗号処理部4 0 1との双方を用いてトリプルDES方式に従った暗号処理方法を実行する構成を説明するフローを示す。図5 6では、一例として記録再生器3 0 0からコンテンツデータを記録デバイス4 0 0にダウンロードする際に実行される保存鍵K s t rを用いたコンテンツ鍵K c o nの暗号化処理例であり、コンテンツ鍵K c o nがトリプルDES方式による鍵である場合の例を示している。なお、ここでは、コンテンツ鍵K c o nを代表して、その処理例を示すが、他の鍵、またはコンテンツ等、その他のデータについても同様の処理が可能である。

トリプルDES方式においては、先の図8～1 0において説明したように、シ

シングルDESでは64ビット鍵、トリプルDES方式による場合は、128ビット、または192ビット鍵構成として、2つ、または3つの鍵が用いられる処理である。これら3つのコンテンツ鍵をそれぞれKcon1, Kcon2, (Kcon3)とする。Kcon3は用いられない場合もあるので、かっこで示している。

図56の処理について説明する。ステップS301は記録再生器300と、記録デバイス400間での相互認証処理ステップである。この相互認証処理ステップは、先に説明した図20の処理によって実行される。なお、この認証処理の際、セッション鍵Ksesが生成される。

ステップS301の認証処理が終了すると、ステップS302において、各チェック値、チェック値A、チェック値B、コンテンツチェック値、総チェック値、各ICVの照合処理が実行される。

これらのチェック値(ICV)照合処理が終了し、データ改竄がないと判定されると、ステップS303に進み、記録再生器300において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308を使って、先に取り出したまたは生成した配送鍵Kdisを用いて、受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたコンテンツ鍵Kconの復号化処理を行う。この場合のコンテンツ鍵は、トリプルDES方式による鍵であり、コンテンツ鍵Kcon1, Kcon2; (Kcon3)である。

次に、ステップS304において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308において、ステップS303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon1のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。

記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたコンテンツ鍵Kcon1を含むデータを記録再生器300の記録再生器暗号処理部

302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

次に、ステップS305において、記録再生器300から送信されてきたコンテンツ鍵Kcon1を受信した記録デバイス400は、受信したコンテンツ鍵Kcon1を記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化する。さらに、ステップS306において、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再暗号化させて、通信部404を介して記録再生器300に送信する。

次に、ステップS307において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308において、ステップS303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon2のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。

記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたコンテンツ鍵Kcon2を含むデータを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

次に、ステップS308において、記録再生器300から送信されてきたコンテンツ鍵Kcon2を受信した記録デバイス400は、受信したコンテンツ鍵Kcon2を記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化する。さらに、ステップS309において、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再暗号化させて、通信部404を介して記録再生器300に送信する。

次に、ステップS310において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308において、ステップ

S 3 0 3 で復号化したコンテンツ鍵 K_{con1} , K_{con2} , (K_{con3}) の中のコンテンツ鍵 K_{con3} のみを相互認証の際に共有しておいたセッション鍵 K_{ses} で暗号化する。

記録再生器 3 0 0 の制御部 3 0 1 は、セッション鍵 K_{ses} で暗号化されたコンテンツ鍵 K_{con3} を含むデータを記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 から読み出し、これらのデータを記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介して記録デバイス 4 0 0 に送信する。

次に、ステップ S 3 1 1 において、記録再生器 3 0 0 から送信されてきたコンテンツ鍵 K_{con3} を受信した記録デバイス 4 0 0 は、受信したコンテンツ鍵 K_{con3} を記録デバイス暗号処理部 4 0 1 の暗号／復号化部 4 0 6 に、相互認証の際に共有しておいたセッション鍵 K_{ses} で復号化する。さらに、ステップ S 3 1 2 において、記録デバイス暗号処理部 4 0 1 の内部メモリ 4 0 5 に保存してある記録デバイス固有の保存鍵 K_{str} で再暗号化させて、通信部 4 0 4 を介して記録再生器 3 0 0 に送信する。

次にステップ S 3 1 3 において、記録再生器の暗号処理部は、図 3 2 ～ 3 5 で説明した各種のデータフォーマットを形成して、記録デバイス 4 0 0 に送信する。

最後にステップ S 3 1 4 において、記録デバイス 4 0 0 は、フォーマット形成が終了した受信データを外部メモリ 4 0 2 に格納する。このフォーマットデータには、保存鍵 K_{str} で暗号化されたコンテンツ鍵 K_{con1} , K_{con2} , (K_{con3}) を含んでいる。

このような処理を実行することにより、記録デバイス 4 0 0 に格納するコンテンツ鍵をトリプル DES 方式の暗号方式による鍵として格納することが可能となる。なお、コンテンツ鍵が K_{con1} , K_{con2} の 2 つの鍵である場合は、ステップ S 3 1 0 ～ S 3 1 2 の処理は省略される。

このように、記録デバイス 4 0 0 は、同じ態様の処理、すなわちステップ S 3 0 5, S 3 0 6 の処理ステップを複数回、その対象を変更するのみで繰り返し実

行することにより、トリプルDESの適用された鍵をメモリに格納可能となる。コンテンツ鍵K_{con}がシングルDESの適用鍵である場合は、ステップS305, S306を実行して、ステップS313のフォーマット化処理を実行してメモリに格納すればよい。このような構成は、ステップS305, S306の処理を実行するコマンドを先に説明した図29のコマンドレジスタに格納し、この処理をコンテンツ鍵の態様、すなわちトリプルDES方式か、シングルDES方式かによって、適宜1回～3回実行する構成とすればよい。従って、記録デバイス400の処理ロジック中にトリプルDESの処理方式を含ませることなく、トリプルDES方式、シングルDES方式、の双方の処理が可能となる。なお、暗号化方式については、コンテンツデータのヘッダ部内の取扱方針に記録し、これを参照することで判定することが可能である。

(14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理

先に説明した図4～6のコンテンツデータ構成から理解されるように、本発明のデータ処理装置において利用されるコンテンツデータのヘッダ部に格納された取扱方針には、コンテンツタイプ、起動優先順位情報が含まれる。本発明のデータ処理装置における記録再生器300は、記録デバイス400、あるいは、DVD、CD、ハードディスク、さらにはゲームカートリッジ等の各種記録媒体に記録されたアクセス可能なコンテンツデータが複数存在する場合、これらコンテンツの起動順位を起動優先順位情報に従って決定する。

記録再生器300は、各記録デバイスDVD装置、CDドライブ装置、ハードディスクドライブ装置等各種記録デバイスとの認証処理を実行後、コンテンツデータ中の優先順位情報に従って、最も優先順位の高いコンテンツデータ中のプログラムを優先して実行する。以下、この「コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」について説明する。

上述した本発明のデータ処理装置実施例の説明においては、記録再生器300が1つの記録デバイス400からコンテンツデータを再生、実行する場合の処理

を中心として説明した。しかし、一般に記録再生器 300 は、図 2 に示すように記録デバイス 400 の他に、読み取り部 304 を介して DVD、CD、ハードディスク、さらに、PIO111、SIO112 を介して接続されるメモリカード、ゲームカートリッジ等、各種記録媒体にアクセス可能な構成を有する。なお、図 2 では、図の複雑化を避けるため読み取り部 304 を 1 つのみ記載しているが、記録再生器 300 は、異なる記憶媒体、例えば DVD、CD、フロッピーディスク、ハードディスクを並列に装着可能である。

記録再生器 300 は、複数の記憶媒体にアクセス可能であり、それぞれの記憶媒体にはそれぞれコンテンツデータが格納されている。例えば CD 等外部のコンテンツプロバイダが供給するコンテンツデータは、前述の図 4 のデータ構成でメディアに格納され、これらのメディアまたは、通信手段を介してダウンロードした場合には、図 26、図 27 のコンテンツデータ構成でメモリカード等の各記憶媒体に格納されている。さらに、具体的には、コンテンツデータのフォーマットタイプに応じて図 32～35 に示すようにメディア上、記録デバイス上でそれぞれ異なるフォーマットで格納される。しかし、いずれの場合にもコンテンツデータのヘッダ中の取扱方針にはコンテンツタイプ、起動優先順位情報が含まれる。

これら、複数のコンテンツデータに対するアクセスが可能な場合の記録再生器のコンテンツ起動処理をフローに従って説明する。

図 57 は、起動可能コンテンツが複数ある場合の処理例 (1) を示す処理フローである。ステップ S611 は、記録再生器 300 がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能な記録デバイスには、メモリカード、DVD 装置、CD ドライブ、ハードディスク装置、さらに、例えば PIO111、SIO112 を介して接続されるゲームカートリッジ等が含まれる。認証処理は、図 2 で示す制御部 301 の制御のもとに各記録デバイスに対して例えば先に図 20 で説明した手順に従って実行される。

次に、ステップ S612 おいて、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体

的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

次に、ステップS 6 1 3において、ステップS 6 1 2で抽出された起動可能なプログラムにおける起動優先順位を判定する。これは、具体的には、ステップS 6 1 2において選択された複数の起動可能なコンテンツデータのヘッダ中の取扱情報に含まれる優先情報を比較して最も高い優先順位を選択する処理である。

次にステップS 6 1 4で選択されたプログラムを起動する。なお、複数の起動可能なプログラムにおいて設定された優先順位が同じである場合には、記録デバイス間でデフォルトの優先順位を設定し、最優先されるデバイスに格納されたコンテンツプログラムを実行する。

図5 8には、複数の記録デバイスに識別子を設定し、各識別子の付された記録デバイスについて順次、認証処理、コンテンツプログラム検索を実行する処理態様、すなわち起動可能コンテンツが複数ある場合の処理例(2)を示した。

ステップS 6 2 1では、記録再生器3 0 0に装着された記録デバイス(i)の認証処理(図2 0参照)を実行するステップである。複数(n個)の記録デバイスには順次1~nの識別子が付与されている。

ステップS 6 2 2では、ステップS 6 2 1での認証が成功したか否かを判定し、認証が成功した場合は、ステップS 6 2 3に進み、その記録デバイス(i)の記録媒体中から起動可能プログラムを検索する。認証が成功しなかった場合は、ステップS 6 2 7に進み、新たなコンテンツ検索可能な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS 6 2 8に進み記録デバイス識別子iを更新し、ステップS 6 2 1以降の認証処理ステップを繰り返す。

ステップS 6 2 3における処理は、記録デバイス(i)に格納されたコンテンツデータから起動可能なプログラムを検出する処理である。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

ステップS 6 2 4では、コンテンツタイプがプログラムであるものが抽出されたか否かを判定し、抽出された場合は、ステップS 6 2 5において、抽出プログラム中最も優先順位の高いものを選択し、ステップS 6 2 6において選択プログラムを実行する。

ステップS 6 2 4において、コンテンツタイプがプログラムであるものが抽出されなかったと判定された場合には、ステップS 6 2 7に進み、新たなコンテンツ検索な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS 6 2 8に進み記録デバイス識別子 i を更新し、ステップS 6 2 1以降の認証処理ステップを繰り返す。

図59は、起動可能コンテンツが複数ある場合の処理例(3)を示す処理フローである。ステップS 6 5 1は、記録再生器300がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能なDVD装置、CDドライブ、ハードディスク装置、メモリカード、ゲームカートリッジ等の認証処理を実行する。認証処理は、図2で示す制御部301の制御のもとに各記録デバイスに対して例えば先に図20で説明した手順に従って実行される。

次に、ステップS 6 5 2において、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

次に、ステップS 6 5 3において、ステップS 6 5 2で抽出された起動可能なプログラムの名称等の情報を表示手段に表示する。なお、表示手段は図2では示されていないが、AV出力データとして出力されたデータが図示しない表示手段に出力される構成となっている。なお、各コンテンツデータのプログラム名等のユーザ提供情報は、コンテンツデータの識別情報中に格納されており、図2に示すメインCPU106の制御のもとに制御部301を介して認証済みの各コンテンツデータのプログラム名称等、プログラム情報を出力手段に出力する。

次にステップS 6 5 4では、図2に示す入力インタフェース、コントローラ、

マウス、キーボード等の入力手段からのユーザによるプログラム選択入力を入力インタフェース110を介してメインCPU106が受領し、選択入力にしたがって、ステップS655においてユーザ選択プログラムを実行する。

このように本発明のデータ処理装置では、コンテンツデータ中のヘッダ内の取扱情報にプログラム起動優先順位情報を格納し、記録再生器300がこの優先順位に従ってプログラムを起動する、あるいは表示手段に起動プログラム情報を表示してユーザによって選択する構成としたので、ユーザがプログラムを検索する必要がなく、起動に要する時間およびユーザの労力を省くことが可能となる。また、起動可能なプログラムは、すべて記録デバイスの認証処理後に起動、または起動可能プログラムであることの表示がなされるので、プログラムを選択してから正当性の確認を行なう等の処理の煩雑性が解消される。

(15) コンテンツ構成および再生(伸長)処理

本発明のデータ処理装置では、上述したように記録再生器300は、メディア500または通信手段600からコンテンツをダウンロード、あるいは記録デバイス400から再生処理を行う。上記の説明は、コンテンツのダウンロード、あるいは再生処理に伴う、暗号化データの処理を中心として説明してきた。

図3の記録再生器300における制御部301は、コンテンツデータを提供するDVD等のデバイス500、通信手段600、記録デバイスからのコンテンツデータのダウンロード処理、または再生処理に伴う認証処理、暗号化、復号化処理全般を制御する。

これらの処理結果として得られた再生可能なコンテンツは、例えば音声データ、画像データ等である。復号データは制御部301から図2に示すメインCPUの制御下に置かれ、音声データ、画像データ等に応じてAV出力部に出力される。しかし、コンテンツが例えば音声データであってMP3圧縮がなされていれば、図2に示すAV出力部のMP3デコーダによって音声データの復号処理がなされて出力される。また、コンテンツデータが画像データであり、MPEG2圧縮画像であれば、AV処理部のMPEG2デコーダによって伸長処理が実行されて

出力されることになる。このように、コンテンツデータに含まれるデータは、圧縮（符号化）処理がなされている場合もあり、また圧縮処理の施されていないデータもあり、コンテンツに応じた処理を施して出力する。

しかしながら、圧縮処理、伸長処理プログラムには、様々な種類があり、コンテンツプロバイダから圧縮データを提供されても対応する伸長処理実行プログラムが無い場合は、これを再生することができないという事態が発生する。

そこで、本発明のデータ処理装置は、データコンテンツ中に、圧縮データとその復号（伸長）処理プログラムを併せて格納する構成、あるいは圧縮データと復号（伸長）処理プログラムとのリンク情報をコンテンツデータのヘッダ情報として格納する構成を開示する。

図2に示したデータ処理全体図から、本構成に関する要素および関連要素を簡潔にまとめた図を図60に示す。記録再生器300は、例えばDVD、CD等のデバイス500、または通信手段600、あるいはコンテンツを格納したメモリカード等の記録デバイス400から様々なコンテンツの提供を受ける。これらのコンテンツは、音声データ、静止画像、動画像データ、プログラムデータ等であり、また暗号化処理の施されているもの、施されていないもの、また、圧縮処理がなされているもの、なされていないもの等、様々なデータが含まれる。

受領コンテンツが暗号化されている場合は、すでに上述した項目中で説明したような手法によって制御部301の制御、および暗号処理部302の暗号処理によって復号処理が実行される。復号されたデータはメインCPU106の制御下で、AV処理部に109に転送されて、AV処理部109のメモリ3090に格納された後、コンテンツ解析部3091においてコンテンツ構成の解析が実行される。例えばコンテンツ中にデータ伸長プログラムが格納されていれば、プログラム記憶部3093にプログラムを格納し、音声データ、画像データ等のデータが含まれていればこれらをデータ記憶部3092に記憶する。伸長処理部3094では、プログラム記憶部に記憶された例えばMP3等の伸長処理プログラムを用いてデータ記憶部3092に記憶された圧縮データの伸長処理を実行して、ス

スピーカ 3001、モニタ 3002 に出力される。

次に、AV 処理部 109 が制御部 301 を介して受領するデータの構成および処理のいくつかの例について説明する。なお、ここでは、コンテンツの例として音声データを示し、また圧縮プログラムの例として MP3 を適用したものを代表して説明するが、本構成は、音声データのみならず、画像データにも適用できるものであり、また、圧縮伸長処理プログラムについても MP3 のみならず、MP EG 2, 4 等各種のプログラムを適用することが可能である。

図 61 にコンテンツ構成例を示す。図 61 は MP3 によって圧縮された音楽データ 6102、MP3 復号（伸長）処理プログラム 6101 を併せて 1 つのコンテンツとして構成した例である。これらのコンテンツは、1 コンテンツとしてメディア 500、あるいは記録デバイス 400 に格納され、または通信手段 600 から配信される。記録再生器 300 は、これらのコンテンツが先に説明した通り、暗号化されているものであれば、暗号処理部 303 によって復号処理を実行した後、AV 処理部 109 に転送される。

AV 処理部 109 のコンテンツ解析部 3091 では、受け取ったコンテンツを解析し、音声データ伸長プログラム（MP3 デコーダ）部と、圧縮音声データ部からなるコンテンツから、音声データ伸長プログラム（MP3 デコーダ）部を取り出してプログラム記憶部 3093 にプログラムを記憶し、圧縮音声データをデータ記憶部 3092 に記憶する。なお、コンテンツ解析部 3091 は、コンテンツとは別に受領したコンテンツ名、コンテンツ構成情報等の情報を受領したり、あるいはコンテンツ内に含まれるデータ名等の識別データ、データ長、データ構成等を示すデータに基づいてコンテンツ解析を実行してもよい。次に、圧縮伸長処理部 3094 は、プログラム記憶部 3093 に記憶された音声データ伸長プログラム（MP3 デコーダ）に従ってデータ記憶部 3092 に記憶された MP3 圧縮音声データの伸長処理を実行して、AV 処理部 109 は伸長した音声データをスピーカ 3001 に出力する。

図 62 に図 61 のコンテンツ構成を持つデータの再生処理の一例を示すフロー

を示す。ステップS 6 7 1は、A V処理部1 0 9のメモリ3 0 9 0に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のデータから取り出し、モニタ3 0 0 2に表示する。ステップS 6 7 2は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース1 1 0を介して受領し、C P U 1 0 6の制御のもとにユーザ入力データに基づく再生処理命令をA V処理部1 0 9に出力する。A V処理部1 0 9は、ステップS 6 7 3においてユーザ選択によるデータの抽出、伸長処理を実行する。

次に図6 3に、1つのコンテンツには圧縮音声データ、あるいは伸長処理プログラムのいずれか一方が含まれ、さらに各コンテンツのヘッダ情報としてコンテンツの内容を示すコンテンツ情報が含まれる構成例を示す。

図6 3に示すように、コンテンツがプログラム6 2 0 2である場合は、ヘッダ情報6 2 0 1としてプログラムであること、およびプログラム種類がMP 3伸長プログラムであることを示すコンテンツ識別情報が含まれる。一方、音声データ6 2 0 4をコンテンツとして含む場合は、ヘッダ6 2 0 3のコンテンツ情報にはMP 3圧縮データであるとの情報が含まれる。このヘッダ情報は、前述した例えば図4に示すコンテンツデータ構成の取扱方針（図5参照）中に含まれるデータから再生に必要な情報のみを選択してA V処理部1 0 9へ転送するコンテンツに付加して構成することが可能である。具体的には、図5に示す「取扱方針」中の各構成データに暗号処理部3 0 2において必要となる取扱方針データと、A V処理部1 0 9における再生処理時に必要となるデータとの識別値を付加し、これら識別値が、A V処理部1 0 9において必要であることを示すもののみを抽出してヘッダ情報とすることができる。

図6 3に示す各コンテンツを受領したA V処理部1 0 9のコンテンツ解析部3 0 9 1は、ヘッダ情報に従って、プログラムである場合はプログラムコンテンツをプログラム記憶部3 0 9 3に記憶し、データである場合は、データコンテンツをデータ記憶部3 0 9 2に記憶する。その後、圧縮伸長処理部3 0 9 4は、デー

タ記憶部からデータを取り出して、プログラム記憶部 3093 に記憶した MP3 プログラムに従って伸長処理を実行して出力する。なお、プログラム記憶部 3093 にすでに同一プログラムが格納されている場合は、プログラム格納処理は省略してもよい。

図 64 に図 63 のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップ S675 は、AV 処理部 109 のメモリ 3090 に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のヘッダから取り出し、モニタ 3002 に表示する。ステップ S676 は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース 110 を介して受領する。

次に、ステップ S677 では、ユーザ選択に対応するデータの再生用プログラム（例えば MP3）を検索する。このプログラム検索対象は、記録再生機器 300 のアクセス可能な範囲を最大検索範囲とすることが好ましく、例えば図 60 に示す、各メディア 500、通信手段 600、記録デバイス 400 等も検索範囲とする。

AV 処理部 109 に渡されるコンテンツはデータ部のみであり、プログラムコンテンツは記録再生器 300 内の他の記録媒体に格納される場合もあり、DVD、CD 等のメディアを介してコンテンツ提供者から提供されることもある。従って、検索対象を記録再生機器 300 のアクセス格納範囲を検索範囲とする。検索の結果として再生プログラムが見つかり、CPU 106 の制御のもとにユーザ入力データに基づく再生処理命令を AV 処理部 109 に出力する。AV 処理部 109 は、ステップ S679 においてユーザ選択によるデータの抽出、伸長処理を実行する。また、別の実施例として、プログラムの検索をステップ S675 より前に行い、ステップ S675 においては、プログラムが検出されたデータのみを表示するようにしてもよい。

次に図 65 に、1 つのコンテンツに圧縮音声データ 6303、伸長処理プログラム 6302 が含まれ、さらにコンテンツのヘッダ情報 6301 としてコンテン

ツの再生優先順位情報が含まれる構成例を示す。これは、先の図 6 1 のコンテンツ構成にヘッダ情報として再生優先順位情報を付加した例である。これは、前述の「(14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」と同様、AV処理部 109 が受領したコンテンツ間において設定された再生優先順位に基づいて再生順を決定するものである。

図 6 6 に図 6 5 のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップ S 6 8 1 は、AV処理部 109 のメモリ 3090 に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部 109 内のメモリの一部領域を使用して設定する。次に、ステップ S 6 8 2 において、AV処理部 109 のコンテンツ解析部 3091 において検索リストから優先順位の高いデータを選択し、ステップ S 6 8 3 において、選択されたデータの再生処理を実行する。

次に図 6 7 に、1つのコンテンツにヘッダ情報とプログラムデータ 6402、あるいはヘッダ情報 6403 と、圧縮データ 6404 のいずれかの組合せから成る例において、データコンテンツのヘッダ 6403 にのみ、再生優先順位情報が付加されている構成例を示す。

図 6 8 に図 6 7 のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップ S 6 9 1 は、AV処理部 109 のメモリ 3090 に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部 109 内のメモリの一部領域を使用して設定する。次に、ステップ S 6 9 2 において、AV処理部 109 のコンテンツ解析部 3091 において検索リストから優先順位の高いデータを選択する。

次に、ステップ S 6 9 3 では、選択されたデータに対応するデータ再生用プログラム（例えばMP3）を検索する。このプログラム検索対象は、先の図 6 4 のフローにおける処理と同様、記録再生機器 300 のアクセス格納範囲を最大検索範囲とすることが好ましく、例えば図 6 0 に示す各メディア 500、通信手段 600、記録デバイス 400 等も検索範囲とする。

検索の結果として再生プログラムが見つかる（ステップS 6 9 4でY e s）と、ステップS 6 9 5において、選択されたデータを検索の結果得られたプログラムを用いて、伸長再生処理を実行する。

一方、検索結果としてプログラムが検出されなかった場合（ステップS 6 9 4でY e s）は、ステップS 6 9 6に進み、ステップS 6 9 1で設定した検索リスト中に含まれる他のデータにおいて、同一のプログラムを用いた再生処理が必要なものを削除する。これは、新たにそのデータに対する再生プログラム検索を実行しても検出されないことが明らかであるからである。さらに、ステップS 6 9 7において検索リストが空であるかを判定し、からでない場合は、ステップS 6 9 2に戻り、さらに次の優先順位の高いデータを抽出して、プログラム検索処理を実行する。

このように、本構成によれば、圧縮処理されたコンテンツは、その復号（伸長）プログラムと共に構成されるか、あるいはコンテンツが圧縮されたデータのみ、あるいは伸長処理プログラムのみである場合は、それぞれのコンテンツにコンテンツがどのような圧縮データであるのか、あるいはどのような処理を実行するかを示すヘッダ情報を有しているので、コンテンツを受領した処理部（例えばA V処理部）は、圧縮データに付属する伸長処理プログラムを用いて伸長再生処理を実行するか、あるいは伸長処理プログラムを圧縮データのヘッダ情報に基づいて検索して、検索の結果得られたプログラムにしたがって伸長再生処理を実行するので、ユーザによるデータの伸長プログラムの選択、検索等の処理が不要となりユーザ負担が軽減され、効率的なデータ再生が可能となる。さらに、ヘッダに再生優先順位情報を有した構成によれば、再生順序を自動設定する構成が可能となり、ユーザによる再生順設定の操作を省略することができる。

なお、上述の実施例では、圧縮音声データコンテンツ、および音声圧縮データの伸長処理プログラムとしてのMP 3を例として説明したが、圧縮データを含むコンテンツ、圧縮画像データの伸長処理プログラムを有するコンテンツであつても本構成は同様に適用可能であり、同様の効果を奏するものである。

(16) セーブデータの生成および記録デバイスへの格納、再生処理

本発明のデータ処理装置は、例えば記録再生器300において実行されるコンテンツがゲームプログラム等である場合等、ゲームプログラムを途中で中断して、所定時間後、新たに再開したい場合には、その中断時点のゲーム状態等をセーブ、すなわち記録デバイスに格納し、これを再開時に読み出してゲームを続行することが可能な構成を持つ。

従来のゲーム機器、パソコン等の記録再生器におけるセーブデータ保存構成は、例えば記録再生器に内蔵、あるいは外付け可能なメモ리카ード、フロッピーディスク、ゲームカートリッジ、あるいはハードディスク等の記憶媒体にセーブデータを保存する構成を持つが、特に、そのセーブデータに対するセキュリティ確保構成を有しておらず、例えばゲームアプリケーションプログラムに共通の仕様でデータのセーブ処理が行われる構成となっている。

従って、例えばある1つの記録再生器Aを用いてセーブされたセーブデータが別のゲームプログラムによって使用されたり、書換えられたりする事態が発生し、従来、セーブデータのセキュリティはほとんど考慮されていなかったのが実状である。

本発明のデータ処理装置は、このようなセーブデータのセキュリティ確保を実現可能とした構成を提供する。例えばあるゲームプログラムのセーブデータは、そのゲームプログラムのみが使用可能な情報に基づいて暗号化して記録デバイスに格納する。あるいは、記録再生器固有の情報に基づいて暗号化して記録デバイスに格納する。これらの手法により、セーブデータの利用を特定の機器、特定のプログラムだけに制限することができ、セーブデータのセキュリティが確保される。以下、本発明のデータ処理装置における「セーブデータの生成および記録デバイスへの格納、再生処理」について説明する。

図69に本発明のデータ処理装置におけるセーブデータ格納処理について説明するブロック図を示す。DVD、CD等のメディア500、あるいは通信手段600からコンテンツが記録再生器300に提供される。提供されるコンテンツは

、先に説明したようにコンテンツ固有の鍵であるコンテンツ鍵 K_{con} によって暗号化されており、記録再生器300は、前述した「(7) 記録再生器から記録デバイスへのダウンロード処理」の欄で説明(図22参照)した処理に従ってコンテンツ鍵を取得して、暗号化コンテンツを復号した後、記録デバイス400に格納する。ここでは、記録再生器300がコンテンツプログラムをメディア、通信手段から復号して再生、実行を行ない、実行の後、得られるセーブデータを外付け、あるいは内蔵のメモ리카ード、ハードディスク等の各種の記録デバイス400A、400B、400Cのいずれかに格納し、再生する処理、あるいはコンテンツを記録デバイス400Aにダウンロードした後、記録デバイス400Aからコンテンツを再生、実行して、そのセーブデータを外付け、あるいは内蔵のメモ리카ード、ハードディスク等の各種の記録デバイス400A、400B、400Cのいずれかに格納する処理記録デバイス400に格納し、再生する処理について説明する。

記録再生器300には、先に説明したように記録再生器識別子 ID_{dev} 、システムに共通な署名鍵であるシステム署名鍵 K_{sys} 、個々の記録再生器に固有の署名鍵である記録再生器署名鍵 K_{dev} 、さらに各種の個別鍵を生成するマスタ鍵を有する。マスタ鍵については、「(12) マスタ鍵に基づく暗号処理鍵生成構成」において、詳しく説明した通り、例えば、配送鍵 K_{dis} 、あるいは認証鍵 K_{ake} 等を生成する鍵である。ここでは、特にマスタ鍵の種類を限定することなく記録再生器300の有するマスタ鍵全般を代表するものとして MK_x として示す。図69の下段には、セーブデータの暗号鍵 K_{sav} の例を示した。セーブデータ暗号鍵 K_{sav} は、セーブデータを各種記録デバイス400A～Cに格納する場合の暗号化処理、そして、各種記録デバイス400A～Cから再生する際の復号処理に用いられる暗号鍵である。図70以下を用いて、セーブデータの格納処理および再生処理の例を説明する。

図70は、コンテンツ固有鍵、システム共通鍵のいずれかを用いてセーブデータを記録デバイス400A～Cいずれかに格納する処理のフロー図である。なお

、各フローにおける処理は記録再生器 300 が実行する処理であり、各フローでセーブデータを格納する記録デバイスは内蔵、外付け記録デバイス 400A～C のいずれかであればよく、いずれかに限定されるものではない。

ステップ S701 は、コンテンツ識別子、例えばゲーム ID を記録再生器 300 が読み出す処理である。これは、先に説明した図 4、26、27、32～35 に示すコンテンツデータ中の識別情報に含まれるデータであり、セーブデータの格納処理命令を図 2 に示す入力インタフェース 110 を介して受領したメイン CPU 106 がコンテンツ識別子の読み取りを制御部 301 に指示する。

制御部 301 は、実行プログラムが DVD、CD-ROM 等、読取部 304 を介して実行されているコンテンツの場合は、読取部 304 を介してコンテンツデータ中のヘッダに含まれる識別情報を取り出し、実行プログラムが、記録デバイス 400 に格納されたコンテンツである場合は、記録デバイスコントローラ 303 を介して識別情報を取り出す。なお、記録再生器 300 がコンテンツプログラムを実行中で、すでに記録再生器中の RAM、その他のアクセス可能な記録媒体にコンテンツ識別子が格納済みである場合は、新たな読み取り処理を実行せずに、読み込み済みデータに含まれる識別情報を利用してもよい。

次に、ステップ S702 は、プログラムの使用制限を行なうか否かによって処理を変更するステップである。プログラム使用制限とは、保存するセーブデータをそのプログラムのみに固有に利用可能とする制限を付するか否かを設定する制限情報であり、プログラムのみに固有に利用可能とする場合は、「プログラム使用制限あり」とし、プログラムに利用を拘束されないセーブデータとする場合を「プログラム使用制限なし」とする。これは、ユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよく、設定された制限情報は、図 69 の記録デバイス 400A～C にデータ管理ファイルとして格納される。

データ管理ファイルの例を図 71 に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限を含むテ

ープルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図69に示す[*IDdev*]である。プログラム使用制限は、上述したように保存するセーブデータをそのプログラムのみに固有に利用可能とす場合、「する」の設定とし、対応プログラムに制限されない利用を可能とする場合「しない」の設定となる。プログラム使用制限は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。

図70に戻り、フローの説明を続ける。ステップS702において、プログラム使用制限について「する」の設定がされている場合は、ステップS703に進む。ステップS703では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵*Kcon*を読み出してコンテンツ固有鍵をセーブデータ暗号鍵*Ksav*とするか、あるいはコンテンツ固有鍵に基づいてセーブデータ暗号鍵*Ksav*を生成する。

一方、ステップS702において、プログラム使用制限について「しない」の設定がされている場合は、ステップS707に進む。ステップS707では、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵*Ksys*を記録再生器300の内部メモリ307から読み出して、システム署名鍵*Ksys*をセーブデータ暗号鍵*Ksav*とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号鍵*Ksav*を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵*Ksav*として使用してもよい。

次に、ステップS704において、ステップS703、またはステップS707で選択、または生成されたセーブデータ暗号化鍵*Ksav*を用いてセーブデータの暗号化処理を実行する。この暗号化処理は、図2における暗号処理部302が例えば前述のDESアルゴリズムを適用して実行する。

ステップS 7 0 4において暗号化処理されたセーブデータは、ステップS 7 0 5において記録デバイスに格納される。セーブデータを格納可能な記録デバイスが図6 9に示すように複数ある場合は、ユーザが記録デバイス4 0 0 A～Cのいずれかをセーブデータ格納先として予め選択する。さらに、ステップS 7 0 6において先に図7 1を用いて説明したデータ管理ファイルに先にステップS 7 0 2で設定したプログラム使用制限情報の書き込み、すなわちプログラム使用制限「する」または「しない」の書き込みを実行する。

以上で、セーブデータの格納処理が終了する。ステップS 7 0 2においてY e s、すなわち「プログラム使用制限する」の選択がなされ、ステップS 7 0 3においてコンテンツ固有鍵に基づいて生成されたセーブデータ暗号化鍵K s a vによって暗号化処理されたセーブデータは、コンテンツ固有鍵情報を持たないコンテンツプログラムによる復号処理が不可能となり、セーブデータは同じコンテンツ鍵情報を有するコンテンツプログラムのみが利用できることになる。ただし、ここでは、セーブデータ暗号化鍵K s a vは記録再生器固有の情報に基いて生成されたものではないので、例えばメモ리카ード等の着脱可能な記録デバイスに格納されたセーブデータは異なる記録再生器においても対応するコンテンツプログラムと共に使用する限り再生可能となる。

また、ステップS 7 0 2においてN o、すなわち「プログラム使用制限しない」の選択がなされ、ステップS 7 0 7においてシステム共通鍵に基づくセーブデータ暗号化鍵K s a vによって暗号化処理されたセーブデータは、コンテンツ識別子が異なるプログラムを用いた場合でも、また、記録再生器が異なっていた場合でも再生して利用することが可能となる。

図7 2は、図7 0のセーブデータ格納処理によって格納されたセーブデータを再生する処理を示したフローである。

ステップS 7 1 1は、コンテンツ識別子、例えばゲームI Dを記録再生器3 0 0が読み出す処理である。これは、先に説明した図7 0のセーブデータ格納処理のステップS 7 0 1と同様の処理であり、コンテンツデータ中の識別情報に含ま

れるデータを読み出す処理である。

次に、ステップS 7 1 2では、図 6 9に示す記録デバイス4 0 0 A～Cから、図 7 1を用いて説明したデータ管理ファイルを読み出し、ステップS 7 1 1において読み出したコンテンツ識別子、および対応して設定された使用プログラム制限情報を抽出する。データ管理ファイルに設定されたプログラム使用制限が「する」であった場合は、ステップS 7 1 4に進み、「しない」であった場合には、ステップS 7 1 7に進む。

ステップS 7 1 4では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵K c o nを読み出してコンテンツ固有鍵をセーブデータ復号化鍵K s a vとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ復号化鍵K s a vを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

一方、ステップS 7 1 2において、データ管理ファイルの設定がプログラム使用制限について「しない」の設定であった場合は、ステップS 7 1 7において、記録再生器3 0 0内に格納されたシステム共通鍵、例えばシステム署名鍵K s y sを記録再生器3 0 0の内部メモリ3 0 7から読み出して、システム署名鍵K s y sをセーブデータ復号化鍵K s a vとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵K s a vを生成する。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

次に、ステップS 7 1 5において、ステップS 7 1 4、またはステップS 7 1 7で選択、または生成されたセーブデータ復号化鍵K s a vを用いてセーブデータの復号化処理を実行し、ステップS 7 1 6において、復号したセーブデータを記録再生器3 0 0において再生、実行する。

以上で、セーブデータの再生処理が終了する。上述のようにデータ管理ファイ

ルに「プログラム使用制限する」の設定がなされている場合は、コンテンツ固有鍵に基づいてセーブデータ復号化鍵が生成され、「プログラム使用制限しない」の設定がある場合はシステム共通鍵に基づいてセーブデータ復号化鍵が生成される。「プログラム使用制限する」の設定がされている場合、使用しているコンテンツのコンテンツ識別子が同じものでないとセーブデータの復号処理の可能な復号化鍵を得ることができないこととなり、セーブデータのセキュリティを高めることが可能となる。

図 7 3、図 7 4 は、コンテンツ識別子を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図 7 3）、セーブデータ再生処理フロー（図 7 4）である。

図 7 3 において、ステップ S 7 2 1 ～ S 7 2 2 は、図 7 0 のステップ S 7 0 1 ～ S 7 0 2 と同様の処理であり、説明を省略する。

図 7 3 のセーブデータ格納処理フローは、ステップ S 7 2 2 において「プログラム使用制限する」の設定を行なった場合、ステップ S 7 2 3 においてコンテンツデータからコンテンツ識別子、すなわちコンテンツ ID を読み出してコンテンツ ID をセーブデータ暗号化鍵 K_{sav} とするか、あるいはコンテンツ ID に基づいてセーブデータ暗号化鍵 K_{sav} を生成する。例えば、記録再生器 3 0 0 の暗号処理部 3 0 7 はコンテンツデータから読み出したコンテンツ ID に、記録再生器 3 0 0 の内部メモリに格納されたマスター鍵 MK_x を適用して、例えば DES (MK_x , コンテンツ ID) によってセーブデータ暗号化鍵 K_{sav} を得ることができる。または、別途、記録再生器 3 0 0 の内部メモリ 3 0 7 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。

一方、ステップ S 7 2 2 において、プログラム使用制限について「しない」の設定とした場合は、ステップ S 7 2 7 において、記録再生器 3 0 0 内に格納されたシステム共通鍵、例えばシステム署名鍵 K_{sys} を記録再生器 3 0 0 の内部メモリ 3 0 7 から読み出して、システム署名鍵 K_{sys} をセーブデータ暗号化鍵 K

s a v とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵 K s a v を生成する。または、別途、記録再生器 3 0 0 の内部メモリ 3 0 7 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵 K s a v として使用してもよい。

ステップ S 7 2 4 以下の処理は、前述の図 7 0 の処理フローにおけるステップ S 7 0 4 以下の処理と同様であり、説明を省略する。

さらに、図 7 4 は、図 7 3 のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップ S 7 3 1 ~ S 7 3 3 は前述の図 7 2 の対応処理と同様であり、ステップ S 7 3 4 のみが異なる。ステップ S 7 3 4 においては、コンテンツデータからコンテンツ識別子、すなわちコンテンツ I D を読み出してコンテンツ I D をセーブデータ復号化鍵 K s a v とするか、あるいはコンテンツ I D に基づいてセーブデータ復号化鍵 K s a v を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ識別子に基づいて暗号化されたデータは、同一のコンテンツ識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

以下の処理、ステップ S 7 3 5、S 7 3 6、S 7 3 7 は、図 7 2 の対応処理と同様であるので説明を省略する。図 7 3、図 7 4 のセーブデータ格納および再生処理に従えば、プログラム使用制限するの設定を行なった場合、コンテンツ I D を使用してセーブデータ暗号化鍵、復号化鍵を生成する構成としたので、先のコンテンツ固有鍵を使用したセーブデータ格納、再生処理と同様、対応するコンテンツプログラムが整合する場合以外は、セーブデータを利用することができない構成となり、セーブデータセキュリティを高めた保存が可能となる。

図 7 5、図 7 7 は、記録再生器固有鍵を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図 7 5）、セーブデータ再生処理フロー（図 7 7）である。

図 7 5 において、ステップ S 7 4 1 は、図 7 0 のステップ S 7 0 1 と同様の処

理であり、説明を省略する。ステップS 7 4 2は、記録再生器の制限をするかしないかを設定するステップである。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。ステップS 7 4 2において「記録再生器制限する」の設定をすると、ステップS 7 4 3に進み、「しない」の設定をするとステップS 7 4 7に進む。

データ管理ファイルの例を図7 6に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、記録再生器制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図6 9に示す[I D d e v] である。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。記録再生器制限情報は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。

図7 5のセーブデータ格納処理フローにおいては、ステップS 7 4 2において「記録再生器制限する」の設定を行なった場合、ステップS 7 4 3において記録再生器3 0 0から記録再生器固有鍵、例えば記録再生器署名鍵K d e vを記録再生器3 0 0の内部メモリ3 0 7から読み出して記録再生器署名鍵K d e vをセーブデータ暗号化鍵K s a vとするか、あるいは記録再生器署名鍵K d e vに基づいてセーブデータ暗号化鍵K s a vを生成する。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

一方、ステップS 7 4 2において、記録再生器制限について「しない」の設定

とした場合は、ステップS 7 4 7において、記録再生器3 0 0内に格納されたシステム共通鍵、例えばシステム署名鍵K s y sを記録再生器3 0 0の内部メモリ3 0 7から読み出して、システム署名鍵K s y sをセーブデータ暗号化鍵K s a vとするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵K s a vを生成する。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

ステップS 7 4 4、S 7 4 5の処理は、前述の図7 0の処理フローにおける対応処理と同様であり、説明を省略する。

ステップS 7 4 6では、データ管理ファイル（図7 6参照）にコンテンツ識別子、記録再生器識別子、そしてステップ7 4 2でユーザが設定した記録再生器制限情報「する／しない」を書き込む。

さらに、図7 7は、図7 5のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップS 7 5 1は前述の図7 2の対応処理と同様、コンテンツ識別子を読み出す。次に、ステップS 7 5 2においては、記録再生器3 0 0内のメモリに格納された記録再生器識別子（I D d e v）を読み出す。

ステップS 7 5 3では、データ管理ファイル（図7 6参照）からコンテンツ識別子、記録再生器識別子、設定済みの記録再生器制限情報「する／しない」の各情報を読み出す。データ管理ファイル中のコンテンツ識別子が一致するエントリにおいて、記録再生器制限情報が「する」に設定されている場合、テーブルエントリの記録再生器識別子がステップS 7 5 2で読み取られた記録再生器識別子と異なる場合は処理を終了する。

次に、ステップS 7 5 4でデータ管理ファイルの設定が「記録再生器制限する」である場合は、ステップS 7 5 5に進み、「しない」である場合は、ステップS 7 5 8に進む。

ステップS 7 5 5においては、記録再生器3 0 0から記録再生器固有鍵、例え

ば記録再生器署名鍵K d e vを記録再生器300の内部メモリ307から読み出して記録再生器署名鍵K d e vをセーブデータ復号化鍵K s a vとするか、あるいは記録再生器署名鍵K d e vに基づいてセーブデータ復号化鍵K s a vを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器固有鍵に基づいて暗号化されたデータは、同一の記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

一方ステップS758においては、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵K s y sを記録再生器300の内部メモリ307から読み出して、システム署名鍵K s y sをセーブデータ復号化鍵K s a vとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵K s a vを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。以下のステップS756、S757は、前述のセーブデータ再生処理フローの対応ステップと同様の処理である。

図75、図77に示すセーブデータ格納、再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器固有鍵によって暗号化、復号化処理が実行されるため、同一の記録再生器固有鍵を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。

次に、図78、図79に記録再生器識別子を用いてセーブデータの暗号化、復号化鍵を生成して格納、再生する処理フローを示す。

図78は、記録再生器識別子を用いてセーブデータの暗号化を行い記録デバイスに格納する。ステップS761～S763は、先の図75と同様の処理である。ステップS764では、記録再生器から読み出した記録再生器識別子（I D d e v）を用いてセーブデータの暗号化鍵K s a vを生成する。I D d e vをセー

ブデータ暗号化鍵 K_{sav} として適用するか、あるいは記録再生器300の内部メモリに格納されたマスター鍵 MK_x を適用して、 $DES(MK_x, IDdev)$ によってセーブデータ暗号化鍵 K_{sav} を得る等、 $IDdev$ に基づいてセーブデータ暗号化鍵 k_{sav} を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。

以下の処理ステップS765～S768は、前述の図75の対応処理と同様であり、説明を省略する。

図79は、図78の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップS771～S774は、前述の図77の対応処理と同様である。

ステップS775では、記録再生器から読み出した記録再生器識別子($IDdev$)を用いてセーブデータの復号化鍵 K_{sav} を生成する。 $IDdev$ をセーブデータ復号化鍵 K_{sav} として適用するか、あるいは記録再生器300の内部メモリに格納されたマスター鍵 MK_x を適用して、 $DES(MK_x, IDdev)$ によってセーブデータ復号化鍵 K_{sav} を得る等、 $IDdev$ に基づいてセーブデータ復号化鍵 K_{sav} を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器識別子に基づいて暗号化されたデータは、同一の記録再生器識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。

以下の処理ステップS776～S778は前述の図76の対応ステップの処理と同様である。

この図78、図79に示すセーブデータ格納、再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再

生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。

次に図80～82を用いて、上述のプログラム使用制限、および記録再生器使用制限を併せて実行するセーブデータ格納、再生処理について説明する。

図80は、セーブデータ格納処理フローである。ステップS781において、コンテンツ識別子をコンテンツデータから読み出し、ステップS782において、プログラム使用制限判定を行ない、ステップS783において記録再生器制限判定を行なう。

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップS785において、コンテンツ固有鍵(ex. Kcon)と、記録再生器固有鍵(Kdev)の双方に基づいてセーブデータ暗号化鍵Ksavが生成される。これは、例えば $Ksav = (Kcon \text{ XOR } Kdev)$ 、あるいは記録再生器300の内部メモリに格納されたマスタ鍵MKxを適用して $Ksav = DES(MKx, Kcon \text{ XOR } Kdev)$ 等によって得ることができる。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。

「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップS786において、コンテンツ固有鍵(ex. Kcon)をセーブデータ暗号化鍵Ksavとするか、あるいはコンテンツ固有鍵(ex. Kcon)に基づいてセーブデータ暗号化鍵Ksavを生成する。

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップS787において、記録再生器固有鍵(Kdev)をセーブデータ暗号化鍵Ksavとするか、あるいは記録再生器固有鍵(Kdev)に基づいてセーブデータ暗号化鍵Ksavが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。

さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、

ステップS 7 8 7において、システム共通鍵、例えばシステム署名鍵K s y sをセーブデータ暗号化鍵K s a vとするか、あるいはシステム署名鍵K s y sに基づいてセーブデータ暗号化鍵K s a vを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

ステップS 7 8 9では、ステップS 7 8 5～S 7 8 8のいずれかで生成されたセーブデータ暗号化鍵K s a vによってセーブデータが暗号化され、記録デバイスに格納される。

さらに、ステップS 7 9 0では、ステップS 7 8 2、S 7 8 3において設定した制限情報がデータ管理ファイルに格納される。データ管理ファイルは、例えば図81に示す構成となり、項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限を含む。

図82は、図80の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップS 7 9 1では、実行プログラムのコンテンツ識別子、記録再生器識別子を読み出し、ステップS 7 9 2において、図81に示すデータ管理ファイルからコンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限情報を読み出す。この場合、プログラム使用制限が「する」でコンテンツ識別子が不一致である場合、または記録再生器制限情報が「する」で記録再生器識別子が不一致である場合は、処理を終了する。

次に、ステップS 7 9 3、S 7 9 4、S 7 9 5では、データ管理ファイルの記録データにしたがって復号鍵生成処理をステップS 7 9 6～S 7 9 9の4態様のいずれかに設定する。

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップS 7 9 6において、コンテンツ固有鍵（ex. K c o n）と、記録再生器固有鍵（K d e v）の双方に基づいてセーブデータ復号化鍵K s a vが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。「プロ

グラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップS 7 9 7において、コンテンツ固有鍵（e x. K c o n）をセーブデータ復号化鍵K s a vとするか、あるいはコンテンツ固有鍵（e x. K c o n）に基づいてセーブデータ復号化鍵K s a vを生成する。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップS 7 9 8において、記録再生器固有鍵（K d e v）をセーブデータ復号化鍵K s a vとするか、あるいは記録再生器固有鍵（K d e v）に基づいてセーブデータ復号化鍵K s a vが生成される。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップS 7 9 9において、システム共通鍵、例えばシステム署名鍵K s y sをセーブデータ復号化鍵K s a vとするか、あるいはシステム署名鍵K s y sに基づいてセーブデータ復号化鍵K s a vを生成する。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

これらの復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

ステップS 8 0 0では、上述のステップS 7 9 6～S 7 9 9のいずれかにおいて生成されたセーブデータ復号化鍵を用いて復号処理が実行され、復号セーブデータが記録再生器3 0 0において再生、実行される。

この図8 0、8 2において示したセーブデータ格納、再生処理フローによれば、「プログラム使用制限する」の選択がなされたセーブデータはコンテンツ固有鍵によって暗号化、復号化処理が実行されるため、同一のコンテンツ固有鍵を持

つコンテンツデータを使用する場合のみ復号して利用することが可能となる。また、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。従って、コンテンツ、記録再生器両者によって利用制限を設定することが可能となり、セーブデータのセキュリティをさらに高めることが可能となる。

なお、図 80、82 においては、コンテンツ固有鍵、記録再生器固有鍵を用いたセーブデータ暗号化鍵、復号化鍵の生成構成を示したが、コンテンツ固有鍵の代わりにコンテンツ識別子、また記録再生器固有鍵の代わりに記録再生器識別子を用いて、これら識別子に基づいてセーブデータ暗号化鍵、復号化鍵の生成を実行する構成としてもよい。

次に、図 83～85 を用いてユーザの入力したパスワードに基づいてセーブデータの暗号化鍵、復号化鍵を生成する構成について説明する。

図 83 はユーザの入力したパスワードに基づいてセーブデータの暗号化鍵を生成して記録デバイスに格納する処理フローである。

ステップ S821 は、コンテンツデータからコンテンツ識別子を読み出す処理であり、前述の各処理と同様である。ステップ S822 は、ユーザによるプログラム使用制限の設定を行なうか否かを決定するステップである。本構成において設定されるデータ管理ファイルは、例えば図 84 に示す構成を持つ。

図 84 に示すように、データは、データ番号、コンテンツ識別子、記録再生器識別子、さらにユーザによるプログラム使用制限情報が含まれる。「ユーザによるプログラム使用制限情報」はプログラムを使用するユーザを制限するかしないかを設定する項目である。

図 83 における処理フローにおけるステップ S822 において使用制限するの設定がなされると、ステップ S823 においてユーザパスワードの入力がなされる。この入力、図 2 に示す例えばキーボード等の入力手段から入力される。

入力されたパスワードは、メインCPU106、制御部301の制御のもとに暗号処理部302に出力され、ステップS824における処理、すなわち入力ユーザパスワードに基づくセーブデータ暗号化鍵Ksavが生成される。セーブデータ暗号化鍵Ksav生成処理としては、例えばパスワード自体を暗号化鍵Ksavとしてもよいし、あるいは記録再生器のマスタ鍵MKxを用いて、セーブデータ暗号化鍵Ksav=DES(MKx, パスワード)によって生成してもよい。また、パスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵を生成してもよい。

ステップS822におけるユーザ制限がNoとされている場合は、ステップS828において、記録再生器300のシステム共通鍵に基づいてセーブデータ暗号化鍵が生成される。

さらに、ステップS825でステップS824、またはステップS828で生成したセーブデータ暗号化鍵Ksavを用いてセーブデータの暗号化処理がなされ、ステップS826において暗号化処理のなされたセーブデータが記録デバイスに格納される。

さらに、ステップS827において、図84のデータ管理ファイルにステップS822で設定したユーザによるプログラム使用制限情報が、コンテンツ識別子と記録再生器識別子に対応付けられて書き込まれる。

図85は、図83の処理によって格納されたセーブデータの再生処理フローを示した図である。ステップS831において、コンテンツデータからコンテンツ識別子を読み出し、ステップS832において図84に示したデータ管理ファイルからコンテンツ識別子、ユーザによるプログラム使用制限情報を読み出す。

ステップS833において、データ管理ファイル中のデータに基づく判定を実行し、「ユーザによるプログラム使用制限する」が設定されている場合は、ステップS834において、パスワード入力を求め、ステップS835において、入力パスワードに基づく復号化鍵を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるパスワードに基づいて暗

号化されたデータは、同一のパスワードに基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムに設定される。

ステップS 8 3 3の判定がユーザによるプログラム使用制限なしの場合は、ステップS 8 3 7において記録再生器3 0 0の内部メモリに格納されたシステム共通鍵、例えばシステム署名鍵K s y sを用いてセーブデータ復号鍵K s a vが生成される。または、別途、記録再生器3 0 0の内部メモリ3 0 7内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K s a vとして使用してもよい。

ステップS 8 3 6では、ステップS 8 3 5、ステップS 8 3 7のいずれかにおいて生成された復号化鍵K s a vを用いて記録デバイスに格納されたセーブデータの復号が実行され、ステップS 8 3 6において記録再生器においてセーブデータの再生、実行がなされる。

図8 3、図8 5において示したセーブデータ格納、再生処理フローによれば、「ユーザによるプログラム使用制限する」の選択がなされたセーブデータはユーザ入力パスワードに基づく鍵によって暗号化、復号化処理が実行されるため、同一のパスワードを入力した場合のみ復号して利用することが可能となり、セーブデータのセキュリティを高めることが可能となる。

以上、いくつかのセーブデータの格納処理、再生処理態様について説明してきたが、上述した処理を融合した処理、例えばパスワードと、記録再生器識別子、コンテンツ識別子等を任意に組み合わせて使用してセーブデータ暗号化鍵、復号化鍵を生成する態様も可能である。

(1 7) 不正機器の排除（リボケーション）構成

すでに説明してきたように、本発明のデータ処理装置においては、メディア5 0 0（図3参照）、通信手段6 0 0から提供される様々なコンテンツデータを記録再生器3 0 0において、認証、暗号化処理等を実行し、記録デバイスに格納する構成によって提供コンテンツのセキュリティを高めるとともに、また、正当な利用者のみが利用可能とする構成を持つ。

上述の説明から理解されるように、入力コンテンツは、記録再生器 300 の暗号処理部 302 に構成される内部メモリ 307 に格納された様々な署名鍵、マスター鍵、チェック値生成鍵（図 18 参照）を用いて、認証処理、暗号化处理、復号化处理がなされる。この鍵情報を格納する内部メモリ 307 は、先に説明したように、基本的に外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされるのが望ましいが、万が一内部メモリの不正な読み取りが実行され、これらの鍵データ等が流出し、正規なライセンスのされていない記録再生器にコピーされた場合、コピーされた鍵情報によって不正なコンテンツ利用がなされる可能性がある。

ここでは、これらの不正コピーによる鍵の複製によるコンテンツの不正利用を防止する構成について説明する。

図 86 に、本構成「(17) 不正機器の排除構成」を説明するブロック図を示す。記録再生器 300 は、前述の図 2, 3 に示す記録再生器と同様であり、内部メモリを有し、先に説明した（図 18）各種の鍵データ、さらに、記録再生器識別子を有している。なお、ここでは、第三者によって複製されている記録再生器識別子、鍵データ等は図 3 に示す内部メモリ 307 に格納されるとは限らず、図 86 に示す記録再生器 300 の鍵データ等は、暗号処理部 302（図 2, 3 参照）によってアクセス可能なメモリ部にまとめて、あるいは分散して格納されている構成であるとする。

不正機器の排除構成を実現するため、コンテンツデータのヘッダ部の不正な記録再生器識別子リストを記憶した構成とした。図 86 に示すように、コンテンツデータには、不正な記録再生器識別子（ID dev）リストとしてのリボケーション（Revocation）リストを保有している。さらに、リボケーションリストの改竄チェック用のリストチェック値 ICV rev を設けている。不正な記録再生器識別子（ID dev）リストは、コンテンツ提供者、または管理者が、

例えば不正コピーの流通状態等から判明した不正な記録再生器の識別子 I D d e v をリスト化したものである。このリボケーションリストは例えば配送鍵 K d i s によって暗号化されて格納してもよい。記録再生器による復号処理については、例えば先の図 2 2 のコンテンツダウンロード処理の態様と同様である。

なお、ここでは、理解を容易にするため、リボケーションリストを単独のデータとして図 8 6 のコンテンツデータ中に示してあるが、例えば先に説明したコンテンツデータのヘッダ部の構成要素である取扱方針（例えば図 3 2 ～ 3 5 参照）中にリボケーションリストを含ませてもよい。この場合は、先に説明したチェック値 I C V a によってリボケーションリストを含む取扱方針データの改竄チェックがなされる。リボケーションリストが取扱方針中に含まれる場合は、チェック値 A : I C V a のチェックによって代替され、記録再生器内のチェック値 A 生成鍵 K i c v a が利用され、チェック値生成鍵 K i c v - r e v を格納する必要はない。

リボケーションリストを単独のデータとしてコンテンツデータ中に含ませる場合は、リボケーションリストの改竄チェック用のリストチェック値 I C V r e v によるリボケーションリストのチェックを実行するとともに、リストチェック値 I C V r e v とコンテンツデータ中の他の部分チェック値とから中間チェック値を生成して中間チェック値の検証処理を行なう構成とする。

リボケーションリストの改竄チェック用のリストチェック値 I C V r e v によるリボケーションリストのチェック手法は、前述の図 2 3、図 2 4 等で説明した I C V a、I C V b 等のチェック値生成処理と同様の方法で実行可能である。すなわち、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存したチェック値生成鍵 K i c v - r e v を鍵とし、コンテンツデータ中に含まれるリボケーションリストをメッセージとして図 2 3、図 2 4 等で説明した I C V 計算方法に従って計算される。計算したチェック値 I C V - r e v' とヘッダ (H e a d e r) 内に格納されたチェック値 : I C V - r e v を比較し、一致していた場合には、改竄が無いと判定する。

リストチェック値 ICV_{rev} を含む中間チェック値は、例えば、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されている総チェック値生成鍵 K_{icvt} を鍵とし、検証した $Header$ 内のチェック値 A 、チェック値 B 、リストチェック値 ICV_{rev} 、さらにフォーマットに応じてコンテンツチェック値を加えたメッセージ列に図 7 他で説明した ICV 計算方法を適用して生成する。

これらのリボケーションリスト、リストチェック値は、DVD、CD 等のメディア 500、通信手段 600 を介して、あるいはメモリカード等の記録デバイス 400 を介して記録再生器 300 に提供される。ここで記録再生器 300 は、正当な鍵データを保有する記録再生器である場合と、不正に複製された識別子 ID を有する場合とがある。

このような構成における不正な記録再生器の排除処理の処理フローを図 87 および図 88 に示す。図 87 は、DVD、CD 等のメディア 500、あるいは通信手段 600 からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フローであり、図 88 は、メモリカード等の記録デバイス 400 からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フローである。

まず、図 87 の処理フローについて説明する。ステップ 901 は、メディアを装着して、コンテンツの提供、すなわち再生処理あるいはダウンロードの要求を行なうステップである。この図 87 に示す処理は、例えば記録再生器に DVD 等のメディアを装着してダウンロード処理等を実行する前のステップとして実行される。ダウンロード処理については、先に図 22 を用いて説明している通りであり、図 22 の処理フローの実行の前ステップとして、あるいは図 22 の処理フロー中に挿入される処理としてこの図 87 の処理が実行される。

記録再生器 300 がネットワーク等の通信手段を介してコンテンツ提供を受けられる場合は、ステップ S911 においてコンテンツ配信サービス側との通信セッションを確立し、その後、ステップ S902 へ進む。

ステップS902では、コンテンツデータのヘッダ部からリボケーションリスト(図86参照)を取得する。このリスト取得処理は、コンテンツがメディア内にある場合は、図3に示す制御部301が読取部304を介してメディアから読み出し、コンテンツが通信手段からである場合は、図3に示す制御部301が通信部305を介してコンテンツ配信側から受信する。

次にステップS903において、制御部301は、暗号処理部302にメディア500または通信手段600から取得したリボケーションリストを暗号処理部302に渡し、チェック値生成処理を実行させる。記録再生器300は、内部にリボケーションチェック値生成鍵 $K_{icv-rev}$ を有し、受領したリボケーションリストをメッセージとしてリボケーションチェック値生成鍵 $K_{icv-rev}$ を適用して、例えば図23、図24等で説明したICV計算方法に従ってチェック値 $ICV-rev'$ を計算し、計算結果とコンテンツデータのヘッダ(Header)内に格納されたチェック値: $ICV-rev$ を比較し、一致していた場合には改竄が無い(ステップS904でYes)と判定する。一致しない場合は、改竄されていると判定され、ステップS909に進み処理エラーとして処理を終了する。

次に、ステップS905において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に総チェック値 $ICVt'$ の計算をさせる。総チェック値 $ICVt'$ は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵 K_{sys} を鍵とし、中間チェック値をDESで暗号化して生成する。なお、各部分チェック値、例えば $ICVa$ 、 $ICVb$ 等の検証処理は、この図87に示す処理フロー中では省略してあるが、先に説明した図39～図45の処理フローと同様の各データフォーマットに応じた部分チェック値の検証が行なわれる。

次に、ステップS906において、生成した総チェック値 $ICVt'$ とヘッダ(Header)内の $ICVt$ を比較し、一致していた場合(ステップS906でYes)には、ステップS907へ進む。一致しない場合は、改竄されている

と判定され、ステップS 9 0 9に進み処理エラーとして処理を終了する。

先に説明したように、総チェック値 I C V t は、I C V a、I C V b、さらに、データフォーマットに応じて各コンテンツブロックのチェック値等、コンテンツデータに含まれる部分チェック値全体をチェックするものであるが、ここでは、これらの部分チェック値にさらに、リボケーションリストの改竄チェック用のリストチェック値 I C V r e v を部分チェック値として加えて、これら全ての改竄を検証する。上述の処理によって生成された総チェック値がヘッダ (H e a d e r) 内に格納されたチェック値：I C V t と一致した場合には、I C V a、I C V b、各コンテンツブロックのチェック値、およびリストチェック値 I C V r e v 全ての改竄はないと判断される。

さらにステップS 9 0 7では、改竄無しと判定されたリボケーションリストと、自己の記録再生器3 0 0に格納された記録再生器識別子 (I D d e v) との比較がなされる。

コンテンツデータから読み出された不正な記録再生器識別子 I D d e v のリストに自己の記録再生器の識別子 I D d e v が含まれている場合は、その記録再生器3 0 0は、不正に複製された鍵データを有していると判定され、ステップS 9 0 9に進み、以後の手続きは中止される。例えば図2 2のコンテンツダウンロード処理の手続きの実行を不可能とする。

ステップS 9 0 7において、不正な記録再生器識別子 I D d e v のリストに自己の記録再生器の識別子 I D d e v が含まれていないと判定された場合には、その記録再生器3 0 0は、正当な鍵データを有していると判定され、ステップS 9 0 8に進み、以後の手続き、例えば、プログラム実行処理、あるいは図2 2等のコンテンツダウンロード処理等が実行可能となる。

図8 8は、メモ리카ード等の記録デバイス4 0 0に格納したコンテンツデータを再生する場合の処理を示す。先に説明したように、メモ리카ード等の記録デバイス4 0 0と記録再生器3 0 0は、図2 0で説明した相互認証処理 (ステップS 9 2 1) が実行される。ステップS 9 2 2において、相互認証OKである場合の

み、ステップS 9 2 3以降の処理に進み、相互認証に失敗した場合は、ステップS 9 3 0のエラーとなり、以降の処理は実行されない。

ステップS 9 2 3では、コンテンツデータのヘッダ部からリボケーションリスト(図8 6参照)を取得する。以降のステップS 9 2 4～S 9 3 0の処理は、先の図8 7における対応処理と同様の処理である。すなわち、リストチェック値によるリストの検証(S 9 2 4, S 9 2 5)、総チェック値による検証(S 9 2 6, S 9 2 7)、リストのエントリと自己の記録再生器識別子ID devとの比較(S 9 2 8)を実行し、コンテンツデータから読み出された不正な記録再生器識別子ID devのリストに自己の記録再生器の識別子ID devが含まれている場合は、その記録再生器3 0 0は、不正に複製された鍵データを有していると判定され、ステップS 9 3 0に進み、以後の手続きは中止される。例えば図2 8に示すコンテンツの再生処理を実行不可能とする。一方、不正な記録再生器識別子ID devのリストに自己の記録再生器の識別子ID devが含まれていないと判定された場合には、その記録再生器3 0 0は、正当な鍵データを有していると判定され、ステップS 9 2 9に進み、以後の手続きが実行可能となる。

このように、本発明のデータ処理装置においては、コンテンツ提供者、または管理者が提供するコンテンツに併せて不正な記録再生器を識別するデータ、すなわち不正な記録再生器識別子ID devをリスト化したリボケーションリストをコンテンツデータのヘッダ部の構成データとして含ませて記録再生器利用者に提供し、記録再生器利用者は、記録再生器によるコンテンツの利用に先立って、自己の記録再生器のメモリに格納された記録再生器識別子ID devと、リストの識別子との照合を実行して一致するデータが存在した場合には、以後の処理を実行させない構成としたので鍵データを複製してメモリに格納した不正な記録再生器によるコンテンツ利用を排除することが可能となる。

(1 8) セキュアチップ構成および製造方法

先に説明したように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7、あるいは記録デバイス4 0 0の内部メモリ4 0 5は、暗号鍵などの重要な情報を保持

しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録再生器暗号処理部 302、記録デバイス暗号処理部 401 は、例えば外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

しかしながら、上述の説明で理解されるように、例えば記録再生器暗号処理部 302 の内部メモリ 307 には記録再生器署名鍵 K_{dev} 等の記録再生器毎に異なるデータを書き込むことが必要となる。また、チップ内の不揮発性の記憶領域、例えばフラッシュメモリ、F e R A M 等にチップ毎の個別情報、例えば識別情報 (I D) や暗号鍵情報を書き込んだ後、例えば製品出荷後におけるデータの再書き込み、読み出しを困難とすることが必要となる。

従来の書き込みデータの読み出し、再書き込み処理を困難とするための手法には、例えばデータ書き込みのコマンドプロトコルを秘密にする。あるいは、チップ上のデータ書き込みコマンドを受け付ける信号線と、製品化した後に利用される通信用の信号線を分離して構成し、基板上のチップに直接信号を送らない限りデータ書き込みコマンドが有効とならないようにする等の手法がある。

しかしながら、このような従来手法を採用しても、記憶素子の専門知識を有するものにとっては、回路を駆動させる設備と技術があれば、チップのデータ書き込み領域に対する信号出力が可能であり、また、たとえデータ書き込みのコマンドプロトコルが秘密であったとしても、プロトコルの解析可能性は常に存在する。

このような、秘密データの改変可能性を保持した暗号処理データの格納素子を流通させることは、暗号処理システム全体を脅かす結果となる。また、データの読み出しを防止するために、データ読み出しコマンド自体を実装しない構成とすることも可能であるが、その場合、正規のデータ書き込みを実行した場合であっても、メモリに対するデータ書き込みが実際に行われたか否かを確認したり、書

き込まれたデータが正確に書き込まれているか否かを判定することが不可能となり、不良なデータ書き込みの行われたチップが供給される可能性が発生する。

これらの従来技術に鑑み、ここでは、例えばフラッシュメモリ、F e R A M等の不揮発性メモリに正確なデータ書き込みを可能とするとともに、データの読み出しを困難にするセキュアチップ構成およびセキュアチップ製造方法を提供する。

図 8 9 に、例えば、前述の記録再生器暗号処理部 3 0 2 または記録デバイス 4 0 0 の暗号処理部 4 0 1 に適用可能なセキュリティチップ構成を示す。図 8 9 (A) はチップの製造過程、すなわちデータの書き込み過程におけるセキュリティチップ構成を示し、図 8 9 (B) は、データを書き込んだセキュリティチップを搭載した製品の構成例、例えば記録再生器 3 0 0 、記録デバイス 4 0 0 の例を示す。

製造過程にあるセキュリティチップは、処理部 8 0 0 1 にモード指定用信号線 8 0 0 3 、および各種コマンド信号線 8 0 0 4 が接続され、処理部 8 0 0 1 は、モード指定用信号線 8 0 0 3 で設定されたモード、例えばデータ書き込みモードまたはデータ読み出しモードに応じて不揮発性メモリである記憶部 8 0 0 2 へのデータ書き込み処理、または記憶部 8 0 0 2 からのデータ読み出し処理を実行する。

一方、図 8 9 (B) のセキュリティチップ搭載製品においては、セキュリティチップと外部接続インタフェース、周辺機器、他の素子等とが汎用信号線で接続されるが、モード信号線 8 0 0 3 は、非接続状態とされる。具体的な処理は、例えばモード信号線 8 0 0 3 をグランド接続する、V c c に釣り上げる、信号線をカットする、あるいは絶縁体樹脂で封印する等である。このような処理により、製品出荷後は、セキュリティチップのモード信号線に対するアクセスが困難になり、外部からチップのデータを読み出したり書き込みを行なったりすることの困難性を高めることができる。

さらに、本構成のセキュリティチップ 8 0 0 0 は、データの記憶部 8 0 0 2 に

対する書き込み処理、および記憶部 8002 に書き込まれたデータの読み出し処理を困難にする構成を持ち、たとえ第三者がモード信号線 8003 のアクセスに成功した場合であっても不正なデータ書き込み、読み出しを防止可能である。図 90 に本構成を有するセキュリティチップにおけるデータ書き込みまたは読み出し処理フローを示す。

ステップ S951 は、モード信号線 8003 をデータ書き込みモードまたはデータ読み出しモードに設定するステップである。

ステップ S952 は、チップから認証用情報を取り出すステップである。本構成のセキュリティチップには、例えばワイヤ (Wire)、マスク ROM 構成により、予めパスワード、暗号技術における認証処理用の鍵情報等、認証処理に必要な情報が格納される。ステップ S952 は、この認証情報を読み出して認証処理を実行する。例えば正規なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証 OK (ステップ S953 において Yes) の結果が得られるが、不正なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証に失敗 (ステップ S953 において No) し、その時点で処理が中止される。認証処理は、例えば先に説明した図 13 の相互認証処理手続きに従って実行可能である。図 89 に示す処理部 8001 は、これらの認証処理を実行可能な構成を有する。これは、例えば先に説明した図 29 に示す記録デバイス 400 の暗号処理部 401 の制御部 403 に組み込まれたコマンドレジスタと同様の構成により実現可能である。例えば図 89 のチップの処理部は、図 29 に示す記録デバイス 400 の暗号処理部 401 の制御部 403 に組み込まれたコマンドレジスタと同様の構成を持ち、各種コマンド信号線 8004 に接続された機器から所定のコマンド No が入力されると、対応する処理を実行し、認証処理シーケンスを実行することが可能となる。

処理部 8001 は認証処理において認証がなされた場合にのみ、データの書き込みコマンド、またはデータの読み出しコマンドを受け付けてデータの書き込み

処理（ステップS 9 5 5）、またはデータの読み出し処理（ステップS 9 5 6）を実行する。

このように本構成のセキュリティチップにおいては、データの書き込み時、読み出し時に認証処理を実行する構成としたので、正当な権利を持たない第三者によるセキュリティチップの記憶部からデータの読み出し、または記憶部へのデータ書き込みを防止することができる。

次に、さらに、セキュリティの高い素子構成とした実施例を図 9 1 に示す。この例では、セキュリティチップの記憶部 8 2 0 0 が 2 つの領域に分離され、一方はデータの読み書きが可能な読み出し書き込み併用領域（RW: R e a d W r i t e 領域） 8 2 0 1 であり、他方はデータの書き込みのみが可能な書き込み専用領域（WO: W r i t e O n l y 領域） 8 2 0 2 である。

この構成において、書き込み専用領域（WO: W r i t e O n l y 領域） 8 2 0 2 には、暗号鍵データ、識別子データ等のセキュリティ要請の高いデータを書き込み、一方セキュリティ度のさほど高くない、例えばチェック用のデータ等を読み出し書き込み併用領域（RW: R e a d W r i t e 領域） 8 2 0 1 に書き込む。

処理部 8 0 0 1 は、読み出し書き込み併用領域（RW: R e a d W r i t e 領域） 8 2 0 1 からのデータ読み出し処理は、前述の図 9 0 で説明した認証処理を伴うデータ読み出し処理を実行する。しかし、データ書き込み処理は、図 9 2 のフローに従って実行する。

図 9 2 のステップ S 9 6 1 は、モード信号線 8 0 0 3 を書き込みモードに設定するステップであり、ステップ 9 6 2 では、先の図 9 0 で説明したと同様の認証処理を実行する。認証処理で認証がなされると、ステップ S 9 6 3 に進み、コマンド信号線 8 0 0 4 を介して、書き込み専用（WO）領域 8 2 0 2 にセキュリティの高い鍵データ等の情報の書き込み、読み出し書き込み併用領域（RW: R e a d W r i t e 領域） 8 2 0 1 にセキュリティ度のさほど高くない、例えばチェック用データ書き込むコマンドを処理部 8 0 0 1 に対して出力する。

ステップS 9 6 4 ではコマンドを受領した処理部 8 0 0 1 が、コマンドに応じたデータ書き込み処理をそれぞれ書き込み専用 (W O) 領域 8 2 0 2、読み出し書き込み併用領域 (R W : R e a d W r i t e 領域) 8 2 0 1 に対して実行する。

また、書き込み専用 (W O) 領域 8 2 0 2 に書き込まれたデータの検証処理フローを図 9 3 に示す。

図 9 3 のステップ S 9 7 1 は、処理部 8 0 0 1 において、書き込み専用 (W O) 領域 8 2 0 2 に書き込まれたデータに基づく暗号処理を実行させる。これらの実行構成は、先の認証処理実行構成と同様、コマンドレジスタに格納された暗号処理シーケンスを順次実行する構成によって実現される。また、処理部 8 0 0 1 において実行される暗号処理アルゴリズムは特に限定されるものではなく、例えば先に説明した D E S アルゴリズムを実行する構成とすることができる。

次に、ステップ S 9 7 2 で、セキュリティチップに接続された検証装置が処理部 8 0 0 1 から暗号処理結果を受信する。次に、ステップ S 9 7 3 において、先に記憶部に書き込み処理を行なった正規な書き込みデータに対して処理部 8 0 0 1 において実行されたアルゴリズムと同様の暗号化処理を適用して得た結果と、処理部 8 0 0 1 からの暗号化結果とを比較する。

比較した結果が同一であれば、書き込み専用 (W O) 領域 8 2 0 2 に書き込まれたデータは正しいことが検証される。

この構成では、認証処理が破られて読み出しコマンドが万が一実行可能となっても、データの読み出し可能領域は、読み出し書き込み併用領域 (R W : R e a d W r i t e 領域) 8 2 0 1 に限定され、書き込み専用 (W O) 領域 8 2 0 2 に書き込まれたデータの読み出しは、不可能であり、さらにセキュリティの高い構成となる。また、全く読み出しを不可能としたチップと異なり、読み出し書き込み併用領域 (R W : R e a d W r i t e 領域) 8 2 0 1 が構成されているのでメモリアクセスの正否チェックが可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしな

がら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。また、上記した実施例ではコンテンツの記録、再生を可能な記録再生器を例にして説明してきたが、データ記録のみ、データ再生のみ可能な装置においても本発明の構成は適用可能なものであり、本発明はパーソナルコンピュータ、ゲーム機器、その他の各種データ処理装置一般において実施可能なものである。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

産業上の利用の可能性

本発明は、DVD、CD等の記憶媒体、あるいはCATV、インターネット、衛星通信等の有線、無線各通信手段等の経路で入手可能な音声、画像、ゲーム、プログラム等の各種コンテンツを、ユーザの所有する記録再生器において再生し、専用の記録デバイス、例えばメモ리카ード、ハードディスク、CD-R等に格納するとともに、記録デバイスに格納されたコンテンツを利用する際、コンテンツ配信側の希望する利用制限を付す構成を実現するとともに、この配布されたコンテンツを、正規ユーザ以外の第三者に不正利用されないようにセキュリティを確保する装置及びシステムに利用できる。

請 求 の 範 囲

1. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、

上記コンテンツデータに対する暗号処理を実行する暗号処理部と、

上記暗号処理部に対する制御を実行する制御部とを有し、

上記暗号処理部は、

コンテンツデータ構成部を複数部分に分割した部分データを1以上含む部分データ集合に対するチェック値として部分チェック値を生成し、該生成した部分チェック値の照合処理により上記部分データの検証処理を実行するとともに、

少なくとも上記部分チェック値を1以上含む部分チェック値集合データ列に基づいて中間チェック値を生成し、該生成した中間チェック値を用いて、上記部分チェック値集合を構成する複数の部分チェック値に対応する複数の部分データ集合全体に対する検証処理を実行する構成を有することを特徴とするデータ処理装置。

2. 上記部分チェック値は、チェック対象となる部分データをメッセージとし、部分チェック値生成鍵を適用した暗号処理によって生成される値であり、

上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとし、総チェック値生成鍵を適用した暗号処理によって生成される値であり、

上記暗号処理部は、上記部分チェック値生成鍵および上記総チェック値生成鍵を格納した構成を有することを特徴とする請求の範囲第1項に記載のデータ処理装置。

3. 上記暗号処理部は、生成する部分チェック値に対応する複数種類の部分チェック値生成鍵を有することを特徴とする請求の範囲第2項に記載のデータ処理装

置。

4. 上記暗号処理はDES暗号処理であり、

上記暗号処理部は、DES暗号処理を実行可能な構成を有することを特徴とする請求の範囲第2項に記載のデータ処理装置。

5. 上記部分チェック値は、チェック対象となる部分データをメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、

上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、

上記暗号処理部は、DES-CBCモードによる暗号処理を実行する構成を有することを特徴とする請求の範囲第1項に記載のデータ処理装置。

6. 上記暗号処理部の有するDES-CBCモードによる暗号処理構成は、処理対象となるメッセージ列の一部においてのみトリプルDESが適用される構成であることを特徴とする請求の範囲第5項に記載のデータ処理装置。

7. 上記データ処理装置は、署名鍵を有し、

上記暗号処理部は、

上記中間チェック値に対して上記署名鍵を適用した暗号処理により生成される値をデータ検証のための照合値として適用する構成であることを特徴とする請求の範囲第1項に記載のデータ処理装置。

8. 上記データ処理装置は、署名鍵として異なる複数の署名鍵を有し、

上記暗号処理部は、

上記コンテンツデータの利用制限態様に応じて上記異なる複数の署名鍵から選択された署名鍵を上記中間チェック値に対する暗号処理に適用してデータ検証のための照合値とする構成を有することを特徴とする請求の範囲第7項に記載のデータ処理装置。

9. 上記データ処理装置は、上記複数の署名鍵として、データ検証処理を実行するシステムの全エンティティに共通の共通署名鍵と、データ検証処理を実行する各々の装置固有の装置固有署名鍵とを有することを特徴とする請求の範囲第8項に記載のデータ処理装置。

10. 上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッダ部分チェック値と、データの一部を構成するコンテンツブロックデータについて生成される1以上のコンテンツチェック値とを含み、

上記暗号処理部は、上記ヘッダ部内データの部分データ集合について1以上のヘッダ部分チェック値を生成して照合処理を実行し、上記コンテンツ部内データの部分データ集合について1以上のコンテンツチェック値を生成して照合処理を実行し、さらに、生成された上記ヘッダ部分チェック値および上記コンテンツチェック値全てに基づいて総チェック値を生成して照合処理を実行することによりデータ検証を実行する構成を有することを特徴とする請求の範囲第1項に記載のデータ処理装置。

11. 上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される1以上のヘッダ部分チェック値を含み、

上記暗号処理部は、上記ヘッダ部内データの部分データ集合について1以上のヘッダ部分チェック値を生成して照合処理を実行し、さらに、生成された上記1以上のヘッダ部分チェック値および上記データの一部を構成するコンテンツプロ

ックデータからなるデータ列に基づいて総チェック値を生成して照合処理を実行することによりデータ検証を実行する構成を有することを特徴とする請求の範囲第1項に記載のデータ処理装置。

12. 上記データ処理装置は、さらに、

上記暗号処理部において正当性検証の実行されたデータを格納する記録デバイスを有することを特徴とする請求の範囲第1項に記載のデータ処理装置。

13. 上記暗号処理部における部分チェック値の照合処理において、照合が成立しなかった場合において、

上記制御部は、上記記録デバイスへの格納処理を中止する構成を有することを特徴とする請求の範囲第12項に記載のデータ処理装置。

14. 上記データ処理装置は、さらに、

上記暗号処理部において正当性検証の実行されたデータを再生する再生処理部を有することを特徴とする請求の範囲第1項に記載のデータ処理装置。

15. 上記データ処理装置は、

上記暗号処理部における部分チェック値の照合処理において、照合が成立しなかった場合において、

上記制御部は、上記再生処理部での再生処理を中止する構成を有することを特徴とする請求の範囲第14項に記載のデータ処理装置。

16. 上記データ処理装置は、

上記暗号処理部における部分チェック値の照合処理において、データのヘッダ部分チェック値の照合処理のみを実行し、ヘッダ部分チェック値の照合が成立したデータを上記再生処理部に転送して再生可能とする制御手段を有することを特

徴とする請求の範囲第 1 4 項に記載のデータ処理装置。

1 7. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、

上記コンテンツデータに対する暗号処理を実行する暗号処理部と、

上記暗号処理部に対する制御を実行する制御部とを有し、

上記暗号処理部は、

検証対象データが暗号化データである場合、該暗号化データの復号処理によって得られる復号データに対して演算処理を実行して得られる演算処理結果データに対して署名鍵を適用した暗号処理を施すことにより、該検証対象データのチェック値を生成する構成を有することを特徴とするデータ処理装置。

1 8. 上記演算処理は、上記暗号化データの復号処理によって得られる復号データを所定バイト単位で排他的論理和演算する処理であることを特徴とする請求の範囲第 1 7 項に記載のデータ処理装置。

1 9. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法において、

コンテンツデータ構成部を複数部分に分割した部分データを 1 以上含む部分データ集合に対するチェック値として部分チェック値を生成し、該生成部分チェック値を照合する処理により上記部分データの検証処理を実行し、

少なくとも上記部分チェック値を 1 以上含む部分チェック値集合データ列に基づいて中間チェック値を生成し、該生成中間チェック値を用いて上記部分チェック値集合を構成する複数の部分チェック値に対応する複数の部分データ集合全体に対する検証処理を実行することを特徴とするデータ処理方法。

2 0. 上記部分チェック値は、チェック対象となる部分データをメッセージとし

、部分チェック値生成鍵を適用した暗号処理によって生成される値であり、

上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとし、総チェック値生成鍵を適用した暗号処理によって生成される値であることを特徴とする請求の範囲第19項に記載のデータ処理方法。

21. 上記部分チェック値は、生成する部分チェック値に対応する異なる種類の部分チェック値生成鍵を適用して生成することを特徴とする請求の範囲第20項に記載のデータ処理方法。

22. 上記暗号処理はDES暗号処理であることを特徴とする請求の範囲第20項に記載のデータ処理方法。

23. 上記部分チェック値は、チェック対象となる部分データをメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、

上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であることを特徴とする請求の範囲第19項に記載のデータ処理方法。

24. 上記データ処理方法において、さらに、

上記中間チェック値に対して署名鍵を適用した暗号処理により生成される値をデータ検証のための照合値として適用することを特徴とする請求の範囲第19項に記載のデータ処理方法。

25. 上記データ処理方法において、

データの利用制限態様に応じて異なる署名鍵を上記中間チェック値に対する暗号処理に適用してデータ検証のための照合値とすることを特徴とする請求の範囲

第 2 4 項に記載のデータ処理方法。

2 6. 上記データ処理方法において、

上記署名鍵として、データ検証処理を実行するシステムの全エンティティに共通の共通署名鍵と、データ検証処理を実行する各々の装置固有の装置固有署名鍵とをデータの利用制限態様に応じて選択して使用することを特徴とする請求の範囲第 2 5 項に記載のデータ処理方法。

2 7. 上記データ処理方法において、

上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される 1 以上のヘッダ部分チェック値と、データの一部を構成するコンテンツ部内データについて生成される 1 以上のコンテンツチェック値とを含み、

データ検証処理は、

上記ヘッダ部内データの部分データ集合について 1 以上のヘッダ部分チェック値を生成して照合処理を実行し、

上記コンテンツ部内データの部分データ集合について 1 以上のコンテンツチェック値を生成して照合処理を実行し、

さらに、生成された上記ヘッダ部分チェック値および上記コンテンツチェック値全てに基づいて総チェック値を生成してデータ検証を実行するものであることを特徴とする請求の範囲第 1 9 項に記載のデータ処理方法。

2 8. 上記データ処理方法において、

上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される 1 以上のヘッダ部分チェック値を含み、

データ検証処理は、

上記ヘッダ部内データの部分データ集合について 1 以上のヘッダ部分チェック値を生成して照合処理を実行し、

さらに、生成された上記 1 以上のヘッダ部分チェック値および上記データの一部を構成するコンテンツブロックデータからなるデータ列に基づいて総チェック値を生成して照合処理を実行することによりデータ検証を実行するものであることを特徴とする請求の範囲第 19 項に記載のデータ処理方法。

29. 上記データ処理方法において、

データの検証後、さらに、検証済みデータを記録デバイスに格納する処理を含むことを特徴とする請求の範囲第 19 項に記載のデータ処理方法。

30. 上記データ処理方法において、

上記部分チェック値の照合処理において、照合が成立しなかった場合において、上記記録デバイスへの格納処理を中止する制御を実行することを特徴とする請求の範囲第 29 項に記載のデータ処理方法。

31. 上記データ処理方法において、

データの検証後、データを再生するデータ再生処理を含むことを特徴とする請求の範囲第 19 項に記載のデータ処理方法。

32. 上記データ処理方法において、

上記部分チェック値の照合処理において、照合が成立しなかった場合において、上記再生処理部での再生処理を中止する制御を実行することを特徴とする請求の範囲第 31 項に記載のデータ処理方法。

33. 上記データ処理方法において、

上記部分チェック値の照合処理において、データのヘッダ部分チェック値の照合処理のみを実行し、ヘッダ部分チェック値の照合が成立したデータを上記再生処理部に転送して再生可能とする制御を実行することを特徴とする請求の範囲第

3 1 項に記載のデータ処理方法。

3 4．記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法であり、

検証対象データが暗号化データである場合、該暗号化データの復号処理によって得られる復号データに対して演算処理を実行し、

上記演算処理によって得られる演算処理結果データに対して署名鍵を適用した暗号処理を実行することにより上記検証対象データのチェック値を生成することを特徴とするデータ処理方法。

3 5．上記演算処理は、上記暗号化データの復号処理によって得られる復号データを所定バイト単位で排他的論理和演算する処理であることを特徴とする請求の範囲第 3 4 項に記載のデータ処理方法。

3 6．データ検証処理のためのデータ検証値付与方法であり、

データを複数部分に分割した部分データを 1 以上含む部分データ集合に対するチェック値として部分チェック値を付与し、

少なくとも上記部分チェック値を 1 以上含む部分チェック値集合データ列に対する検証を行なう中間チェック値を検証対象データに付与することを特徴とするデータ検証値付与方法。

3 7．上記部分チェック値は、チェック対象となる部分データをメッセージとし、部分チェック値生成鍵を適用した暗号処理によって生成される値であり、

上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとし、総チェック値生成鍵を適用した暗号処理によって生成される値であることを特徴とする請求の範囲第 3 6 項に記載のデータ検証値付与方法。

38. 上記部分チェック値は、生成する部分チェック値に対応する異なる種類の部分チェック値生成鍵を適用して生成することを特徴とする請求の範囲第37項に記載のデータ検証値付与方法。

39. 上記暗号処理はDES暗号処理であることを特徴とする請求の範囲第37項に記載のデータ処理方法。

40. 上記部分チェック値は、チェック対象となる部分データをメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であり、

上記中間チェック値は、チェック対象となる部分チェック値集合データ列をメッセージとしてDES-CBCモードにおいて生成されるメッセージ認証符号(MAC)であることを特徴とする請求の範囲第36項に記載のデータ検証値付与方法。

41. 上記データ検証値付与方法において、さらに、

上記中間チェック値に対して署名鍵を適用した暗号処理により生成される値をデータ検証のための照合値として適用することを特徴とする請求の範囲第36項に記載のデータ検証値付与方法。

42. 上記データ検証値付与方法において、

データの利用制限態様に応じて異なる署名鍵を上記中間チェック値に対する暗号処理に適用してデータ検証のための照合値とすることを特徴とする請求の範囲第41項に記載のデータ検証値付与方法。

43. 上記データ検証値付与方法において、

上記署名鍵として、データ検証処理を実行するシステムの全エンティティに共

通の共通署名鍵と、データ検証処理を実行する各々の装置固有の装置固有署名鍵とをデータの利用制限態様に応じて選択して使用するよう設定することを特徴とする請求の範囲第 4 2 項に記載のデータ検証値付与方法。

4 4. 上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される 1 以上のヘッダ部分チェック値と、データの一部を構成するコンテンツ部内データについて生成される 1 以上のコンテンツチェック値とを含み、

上記ヘッダ部分チェック値および上記コンテンツチェック値全てに対する総チェック値を生成してデータ検証を実行するよう設定することを特徴とする請求の範囲第 3 6 項に記載のデータ検証値付与方法。

4 5. 上記部分チェック値は、データの一部を構成するヘッダ部内データについて生成される 1 以上のヘッダ部分チェック値を含み、

上記 1 以上のヘッダ部分チェック値および上記データの一部を構成するコンテンツブロックデータからなるデータ列全てに対する総チェック値を生成してデータ検証を実行するよう設定することを特徴とする請求の範囲第 3 6 項に記載のデータ検証値付与方法。

4 6. データ正当性の検証を実行するデータ検証処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、

データを複数部分に分割した部分データを 1 以上含む部分データ集合に対するチェック値として生成される部分チェック値の照合処理により上記部分データの検証処理を実行するステップと、

上記部分チェック値を複数個組み合わせた部分チェック値集合に基づいて生成される中間チェック値を用いて、上記部分チェック値集合を構成する複数の部分チェック値に対応する複数の部分データ集合全体に対する検証処理を実行するス

テップと、

を含むことを特徴とするプログラム提供媒体。

47. データ処理装置において、

データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理部と、

上記暗号処理に適用する鍵を生成するためのマスター鍵を格納した記憶部とを有し、

上記暗号処理部は、上記暗号処理を実行するに必要な個別鍵を、上記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する構成を有することを特徴とするデータ処理装置。

48. 上記データ処理装置は、記憶媒体または通信媒体を介する転送データに関する暗号処理を行なうデータ処理装置であり、

上記記憶部は、上記転送データの暗号処理に適用する配送鍵K d i s を生成する配送鍵生成用マスター鍵MK d i s を格納し、

上記暗号処理部は、

上記記憶部に格納された配送鍵生成用マスター鍵MK d i s と、上記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行して、上記転送データの配送鍵K d i s を生成する構成を有することを特徴とする請求の範囲第47項に記載のデータ処理装置。

49. 上記データ処理装置は、転送データの転送先あるいは転送元となる外部接続装置の認証処理を行なうデータ処理装置であり、

上記記憶部は、上記外部接続装置の認証鍵K a k e を生成する認証鍵生成用マスター鍵MK a k e を格納し、

上記暗号処理部は、

上記記憶部に格納された認証鍵生成用マスター鍵MK a k e と、上記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、上記外部接続装置の認証鍵K a k e を生成する構成を有することを特徴とする請求の範囲第 4 7 項に記載のデータ処理装置。

50. 上記データ処理装置は、データに対する署名処理を実行するデータ処理装置であり、

上記記憶部は、上記データ処理装置のデータ処理装置署名鍵K d e v を生成する署名鍵生成用マスター鍵MK d e v を格納し、

上記暗号処理部は、

上記記憶部に格納された署名鍵生成用マスター鍵MK d e v と、上記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、上記データ処理装置のデータ処理装置署名鍵K d e v を生成する構成を有することを特徴とする請求の範囲第 4 7 項に記載のデータ処理装置。

51. 暗号処理を実行するに必要な個別鍵を、上記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する個別鍵生成処理は、

暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、上記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする請求の範囲第 4 7 項に記載のデータ処理装置。

52. 上記暗号処理はDESアルゴリズムを適用した暗号処理であることを特徴とする請求の範囲第 5 1 項に記載のデータ処理装置。

53. 複数のデータ処理装置から構成されるデータ処理システムにおいて、

上記複数のデータ処理装置の各々が、データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理に適用する鍵を生成す

るための共通のマスター鍵を有し、

上記複数のデータ処理装置の各々が、上記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて上記暗号処理を実行するに必要な共通の個別鍵を生成する構成を有することを特徴とするデータ処理システム。

54. 上記複数のデータ処理装置は、

コンテンツデータを提供するコンテンツデータ提供装置と、コンテンツデータの利用を行なうコンテンツデータ利用装置によって構成され、

コンテンツデータ提供装置およびコンテンツデータ利用装置の双方が、上記コンテンツデータ提供装置およびコンテンツデータ利用装置間における流通コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵を有し、

上記コンテンツデータ提供装置は、上記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、

上記コンテンツデータ利用装置は、上記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行する構成を有することを特徴とする請求の範囲第53項に記載のデータ処理システム。

55. 上記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と上記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、

上記コンテンツデータ利用装置は、上記コンテンツデータ提供装置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも1つの配送鍵生成用マスター鍵

を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号可能とした構成を有することを特徴とする請求の範囲第54項に記載のデータ処理システム。

56. 上記複数のデータ処理装置の各々に、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するための同一のコンテンツ鍵生成用マスター鍵を格納し、

上記複数のデータ処理装置の1つのデータ処理装置Aにおいて、上記コンテンツ鍵生成用マスター鍵と、該データ処理装置Aの装置識別子とに基づいて生成されたコンテンツ鍵により暗号化され記憶媒体に格納されたコンテンツデータを、

異なるデータ処理装置Bにおいて、上記同一のコンテンツ鍵生成用マスター鍵と、上記データ処理装置Aの装置識別子とに基づいてコンテンツ鍵を生成し、該生成したコンテンツ鍵に基づいて、上記データ処理装置Aにおいて上記記憶媒体に格納した暗号化コンテンツデータの復号処理を実行する構成としたことを特徴とする請求の範囲第53項に記載のデータ処理システム。

57. 上記複数のデータ処理装置は、

ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとによって構成され、

上記ホストデバイスおよびスレーブデバイスの双方が、ホストデバイスとスレーブデバイス間の認証処理に適用する認証鍵生成用マスターを有し、

上記スレーブデバイスは、上記認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成してスレーブデバイス内メモリに格納し、

上記ホストデバイスは、上記認証鍵生成用マスター鍵と、上記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処

理を実行する構成を有することを特徴とする請求の範囲第 53 項に記載のデータ処理システム。

58. データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理を実行するデータ処理方法において、

暗号処理を実行するに必要な個別鍵を、上記暗号処理に適用する鍵を生成するためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、

上記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処理ステップと、

を有することを特徴とするデータ処理方法。

59. 上記データ処理方法において実行するデータ処理は、記憶媒体または通信媒体を介する転送データに関する暗号処理であり、

上記鍵生成ステップは、

転送データの暗号処理に適用する配送鍵 K_{dis} を生成する配送鍵生成用マスター鍵 MK_{dis} と、上記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行し、上記転送データの配送鍵 K_{dis} を生成する配送鍵生成ステップであり、

上記暗号処理ステップは、

上記配送鍵生成ステップにおいて生成した配送鍵 K_{dis} に基づいて転送データの暗号処理を実行するステップであることを特徴とする請求の範囲第 58 項に記載のデータ処理方法。

60. 上記データ処理方法において実行するデータ処理は、転送データの転送先あるいは転送元となる外部接続装置の認証処理であり、

上記鍵生成ステップは、

上記外部接続装置の認証鍵K a k eを生成する認証鍵生成用マスター鍵MK a k eと、上記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、上記外部接続装置の認証鍵K a k eを生成する認証鍵生成ステップであり、

上記暗号処理ステップは、

上記認証鍵生成ステップにおいて生成した認証鍵K a k eに基づいて外部接続装置の認証処理を実行するステップであることを特徴とする請求の範囲第58項に記載のデータ処理方法。

61. 上記データ処理装置において実行するデータ処理は、データに対する署名処理であり、

上記鍵生成ステップは、

上記データ処理装置のデータ処理装置署名鍵K d e vを生成する署名鍵生成用マスター鍵MK d e vと、上記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、上記データ処理装置のデータ処理装置署名鍵K d e vを生成する署名鍵生成ステップであり、

上記暗号処理ステップは、

上記署名鍵生成ステップにおいて生成した署名鍵K d e vに基づいてデータに対する署名処理を実行するステップであることを特徴とする請求の範囲第58項に記載のデータ処理方法。

62. 上記鍵生成ステップは、

暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、上記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする請求の範囲第58項に記載のデータ処理方法。

63. 上記暗号処理はDESアルゴリズムを適用した暗号処理であることを特徴とする請求の範囲第62項に記載のデータ処理方法。

64. コンテンツデータを提供するコンテンツデータ提供装置と、コンテンツデータの利用を行なうコンテンツデータ利用装置とからなるデータ処理システムにおけるデータ処理方法であり、

上記コンテンツデータ提供装置は、コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、

上記コンテンツデータ利用装置は、上記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行することを特徴とするデータ処理方法。

65. 上記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と上記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、

上記コンテンツデータ利用装置は、上記コンテンツデータ提供装置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも1つの配送鍵生成用マスター鍵を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号することを特徴とする請求の範囲第64項に記載のデータ処理方法。

66. 複数のデータ処理装置によって構成されるデータ処理システムにおけるデ

ータ処理方法であり、

上記複数のデータ処理装置中の1つのデータ処理装置Aにおいて、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するためのコンテンツ鍵生成用マスター鍵と、該データ処理装置Aの装置識別子とに基づいて生成されたコンテンツ鍵により暗号化されたコンテンツデータを記憶媒体に格納するステップと、

異なるデータ処理装置Bにおいて、上記データ処理装置Aと同一の上記コンテンツ鍵生成用マスター鍵と上記データ処理装置Aの装置識別子とに基づいて上記コンテンツ鍵と同一のコンテンツ鍵を生成するステップと、

上記データ処理装置Bにおいて生成したコンテンツ鍵により上記記憶媒体に格納したコンテンツデータの復号を行なうステップと、

を有することを特徴とするデータ処理方法。

67. ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとからなるデータ処理システムにおけるデータ処理方法であり、

上記スレーブデバイスは、ホストデバイスとスレーブデバイス間の認証処理に適用する認証鍵を生成するための認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成し、生成した認証鍵を該スレーブデバイス内のメモリに格納し、

上記ホストデバイスは、上記認証鍵生成用マスター鍵と、上記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処理を実行することを特徴とするデータ処理方法。

68. データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、

暗号処理を実行するに必要な個別鍵を、上記暗号処理に適用する鍵を生成する

ためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、

上記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処理ステップと、

を含むことを特徴とするプログラム提供媒体。

69. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、

データ処理装置識別子を格納した記憶部と、

コンテンツデータ中に含まれる不正機器リストを抽出し、該リスト内のエントリと上記記憶部に格納された上記データ処理装置識別子との照合処理を実行するリスト検証部と、

上記照合処理部における照合処理の結果、上記不正機器リスト中に上記データ処理識別子と一致する情報が含まれる場合において、上記コンテンツデータの再生または記録デバイスに対する格納処理少なくともいずれかの処理の実行を中止する制御部と、

を有することを特徴とするデータ処理装置。

70. 上記リスト検証部は、上記コンテンツデータに対する暗号処理を実行する暗号処理部を有し、

上記暗号処理部は、

上記コンテンツデータ中に含まれる不正機器リストのチェック値に基づいて上記不正機器リストの改竄の有無を検証し、該検証により、改竄なしと判定した場合にのみ上記照合処理を実行する構成であることを特徴とする請求の範囲第69項に記載のデータ処理装置。

71. 上記データ処理装置は、不正機器リストチェック値生成鍵を有し、

上記暗号処理部は、

検証対象の不正機器リスト構成データに対して上記不正機器リストチェック値生成鍵を適用した暗号処理を実行して不正機器リストチェック値を生成し、該生成した不正機器リストチェック値と、上記コンテンツデータ中に含まれる不正機器リストのチェック値との照合を実行して上記不正機器リストの改竄の有無を検証する構成であることを特徴とする請求の範囲第70項に記載のデータ処理装置。

72. 上記リスト検証部は、上記コンテンツデータに対する暗号処理を実行する暗号処理部を有し、

上記暗号処理部は、

上記コンテンツデータ中に含まれる暗号化された不正機器リストの復号処理を実行し、該復号処理の結果として得られた不正機器リストについて上記照合処理を実行する構成であることを特徴とする請求の範囲第69項に記載のデータ処理装置。

73. 上記リスト検証部は、

コンテンツデータの転送先または転送元となる記録デバイスとの相互認証処理を実行する暗号処理部を有し、

上記リスト検証部は、

上記暗号処理部によって実行される上記記録デバイスとの相互認証処理による認証が成立したことを条件として、上記コンテンツデータ中に含まれる不正機器リストを抽出し上記記憶部に格納された上記データ処理装置識別子との照合処理を実行する構成であることを特徴とする請求の範囲第69項に記載のデータ処理装置。

74. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行

なうデータ処理方法であり、

コンテンツデータ中に含まれる不正機器リストを抽出するリスト抽出ステップと、

上記リスト抽出ステップによって抽出されたリストに含まれるエントリと、データ処理装置内の記憶部に格納された上記データ処理装置識別子との照合処理を実行する照合処理ステップと、

上記照合処理ステップにおける照合処理の結果、上記不正機器リスト中に上記データ処理識別子と一致する情報が含まれる場合、上記コンテンツデータの再生または記録デバイスに対する格納処理少なくともいずれかの処理の実行を中止するステップと、

を有することを特徴とするデータ処理方法。

75. 上記データ処理方法は、さらに、

上記コンテンツデータ中に含まれる不正機器リストのチェック値に基づいて上記不正機器リストの改竄の有無を検証する検証ステップを含み、

上記照合処理ステップは、

上記検証ステップにより、改竄なしと判定した場合にのみ実行することを特徴とする請求の範囲第74項に記載のデータ処理方法。

76. 上記検証ステップは、

検証対象の不正機器リスト構成データに対して不正機器リストチェック値生成鍵を適用した暗号処理を実行して不正機器リストチェック値を生成するステップと、

生成した不正機器リストチェック値と、上記コンテンツデータ中に含まれる不正機器リストのチェック値との照合を実行して上記不正機器リストの改竄の有無を検証するステップと、

を含むことを特徴とする請求の範囲第75項に記載のデータ処理方法。

77. 上記データ処理方法は、さらに、

上記コンテンツデータ中に含まれる暗号化された不正機器リストの復号処理を実行する復号ステップを含み、

上記照合処理ステップは、

上記復号ステップの結果として得られた不正機器リストについて上記照合処理を実行することを特徴とする請求の範囲第74項に記載のデータ処理方法。

78. 上記データ処理方法は、さらに、

コンテンツデータの転送先または転送元となる記録デバイスとの相互認証処理ステップを含み、

上記照合処理ステップは、

上記相互認証処理ステップによって実行される上記記録デバイスとの相互認証処理による認証が成立したことを条件として上記照合処理を実行することを特徴とする請求の範囲第74項に記載のデータ処理方法。

79. 記憶媒体または通信媒体によって複数の記録再生器に対して提供されるコンテンツデータの生成を行なうコンテンツデータ生成方法であり、

コンテンツデータのヘッダ情報として該コンテンツデータの利用の排除対象となる記録再生器の記録再生器識別子を構成データとした不正機器リストを格納してコンテンツデータとすることを特徴とするコンテンツデータ生成方法。

80. 上記コンテンツデータ生成方法において、さらに、

コンテンツデータのヘッダ情報として、上記不正機器リストの改竄チェック用の不正機器リストチェック値を格納することを特徴とする請求の範囲第79項に記載のコンテンツデータ生成方法。

8 1. 上記コンテンツデータ生成方法において、さらに、

上記不正機器リストを暗号化してコンテンツデータのヘッダ情報中に格納することを特徴とする請求の範囲第 7 9 項に記載のコンテンツデータ生成方法。

8 2. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、

コンテンツデータ中に含まれる不正機器リストを抽出するリスト抽出ステップと、

上記リスト抽出ステップによって抽出されたリストに含まれるエントリと、データ処理装置内の記憶部に格納された上記データ処理装置識別子との照合処理を実行する照合処理ステップと、

上記照合処理ステップにおける照合処理の結果、上記不正機器リスト中に上記データ処理識別子と一致する情報が含まれる場合、上記コンテンツデータの再生または記録デバイスに対する格納処理少なくともいずれかの処理の実行を中止するステップと、

を有することを特徴とするプログラム提供媒体。

8 3. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、

上記コンテンツデータに対する暗号処理を実行する暗号処理部と、

上記暗号処理部に対する制御を実行する制御部と、

上記暗号処理部における暗号処理に使用され、上記コンテンツデータを利用する他のデータ処理装置に共通のシステム共通鍵と、

上記暗号処理部における暗号処理に使用されるデータ処理装置固有の装置固有鍵または該装置個有鍵を生成するための装置固有識別子の少なくともいずれかを有し、

上記暗号処理部は、

上記コンテンツデータの利用態様に応じて上記システム共通鍵、または上記装置固有鍵のいずれかを上記コンテンツデータに適用して暗号処理を実行する構成を有することを特徴とするデータ処理装置。

84. 上記暗号処理部は、

上記コンテンツデータに含まれる利用制限情報に応じて上記システム共通鍵、または上記装置固有鍵のいずれかを上記コンテンツデータに適用して暗号処理を実行する構成を有することを特徴とする請求の範囲第83項に記載のデータ処理装置。

85. 上記データ処理装置は、さらに、

コンテンツデータを記録する記録デバイスを有し、

上記暗号処理部は、

上記コンテンツデータを自己のデータ処理装置のみにおいて使用する利用制限を付する場合、上記コンテンツデータに対して上記装置固有鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成し、

上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能とする場合、上記コンテンツデータに対して上記システム共通鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成する構成を有することを特徴とする請求の範囲第83項に記載のデータ処理装置。

86. 上記データ処理装置は、

データ処理装置固有の署名鍵 K_{dev} 、および複数のデータ処理装置に共通のシステム署名鍵 K_{sys} を有し、

上記暗号処理部は、

上記コンテンツデータを自己のデータ処理装置のみにおいて使用する利用制限

を付して上記記録デバイスに格納する場合、上記コンテンツデータに対して上記装置固有の署名鍵K d e vを適用した暗号処理により装置固有チェック値を生成し、

上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能として上記記録デバイスに格納する場合、上記コンテンツデータに対して上記システム署名鍵K s y sを適用した暗号処理により総チェック値を生成し、

上記制御部は、

上記暗号処理部の生成した上記装置固有チェック値または上記総チェック値のいずれかを上記コンテンツデータと共に上記記録デバイスに格納する制御を実行することを特徴とする請求の範囲第83項に記載のデータ処理装置。

87. 上記データ処理装置は、

データ処理装置固有の署名鍵K d e v、および複数のデータ処理装置に共通のシステム署名鍵K s y sを有し、

上記暗号処理部は、

自己のデータ処理装置のみににおいて使用する利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記装置固有の署名鍵K d e vを適用した暗号処理により装置固有チェック値を生成し、該生成した装置固有チェック値の照合処理を実行し、

自己のデータ処理装置以外の装置においても使用可能とされた利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記システム署名鍵K s y sを適用した暗号処理により総チェック値を生成し、該生成した総チェック値の照合処理を実行し、

上記制御部は、

上記装置固有チェック値の照合が成立した場合、あるいは上記総チェック値の照合が成立した場合にのみコンテンツデータの暗号処理部での処理を続行させて再生可能復号データを生成する構成を有することを特徴とする請求の範囲第83

項に記載のデータ処理装置。

88. 上記データ処理装置は、

記録データ処理装置署名鍵用マスター鍵MK d e v、およびデータ処理装置識別子 I D d e v を有し、

上記暗号処理部は、

上記データ処理装置署名鍵用マスター鍵MK d e v と上記データ処理装置識別子 I D d e v とに基づく暗号処理によりデータ処理装置固有鍵としての署名鍵K d e v を生成する構成を有することを特徴とする請求の範囲第83項に記載のデータ処理装置。

89. 上記暗号処理部は、

上記データ処理装置識別子 I D d e v に対して上記データ処理装置署名鍵用マスター鍵MK d e v を適用したDES暗号処理により上記署名鍵K d e v を生成する構成であることを特徴とする請求の範囲第88項に記載のデータ処理装置。

90. 上記暗号処理部は、

上記コンテンツデータに対する暗号処理を実行して中間チェック値を生成し、該中間チェック値に上記データ処理装置固有鍵またはシステム共有鍵を適用した暗号処理を実行することを特徴とする請求の範囲第83項に記載のデータ処理装置。

91. 上記暗号処理部は、

上記コンテンツデータを複数部分に分割した部分データを1以上含む部分データ集合に対する暗号処理により部分チェック値を生成し、

該生成した部分チェック値を含む部分チェック値集合データ列に対する暗号処理により中間チェック値を生成する構成であることを特徴とする請求の範囲第9

0 項に記載のデータ処理装置。

9 2. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法であり、

上記コンテンツデータの利用態様に応じて、

上記コンテンツデータを利用する他のデータ処理装置に共通の暗号処理用システム共通鍵、または、データ処理装置固有の装置固有鍵のいずれかの暗号処理鍵を選択し、

選択した暗号処理鍵を上記コンテンツデータに適用して暗号処理を実行することを特徴とするデータ処理方法。

9 3. 上記データ処理方法において、

上記暗号処理鍵を選択するステップは、上記コンテンツデータに含まれる利用制限情報に応じて選択するステップであることを特徴とする請求の範囲第 9 2 項に記載のデータ処理方法。

9 4. 上記データ処理方法におけるコンテンツデータの記録デバイスに対する記録処理において、

上記コンテンツデータを自己のデータ処理装置のみにおいて使用する利用制限を付する場合、上記コンテンツデータに対して上記装置固有鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成し、

上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能とする場合、上記コンテンツデータに対して上記システム共通鍵を用いた暗号処理を実行して上記記録デバイスへの格納データを生成することを特徴とする請求の範囲第 9 2 項に記載のデータ処理方法。

9 5. 上記データ処理方法におけるコンテンツデータの記録デバイスに対する記

録処理において、

上記コンテンツデータを自己のデータ処理装置のみにおいて使用する利用制限を付して上記記録デバイスに格納する場合、上記コンテンツデータに対して上記装置固有の署名鍵 K_{dev} を適用した暗号処理により装置固有チェック値を生成し、

上記コンテンツデータを自己のデータ処理装置以外の装置においても使用可能として上記記録デバイスに格納する場合、上記コンテンツデータに対して上記システム署名鍵 K_{sys} を適用した暗号処理により総チェック値を生成し、

上記生成した上記装置固有チェック値または上記総チェック値のいずれかを上記コンテンツデータと共に上記記録デバイスに格納することを特徴とする請求の範囲第 9 2 項に記載のデータ処理方法。

9 6. 上記データ処理方法におけるコンテンツデータの再生処理において、

自己のデータ処理装置のみにおいて使用する利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記装置固有の署名鍵 K_{dev} を適用した暗号処理により装置固有チェック値を生成し、該生成した装置固有チェック値の照合処理を実行し、

自己のデータ処理装置以外の装置においても使用可能とされた利用制限の付されたコンテンツデータを再生する場合、上記コンテンツデータに対して上記システム署名鍵 K_{sys} を適用した暗号処理により総チェック値を生成し、該生成した総チェック値の照合処理を実行し、

上記装置固有チェック値の照合が成立した場合、あるいは上記総チェック値の照合が成立した場合にのみコンテンツデータの再生を実行することを特徴とする請求の範囲第 9 2 項に記載のデータ処理方法。

9 7. 上記データ処理方法において、さらに、

データ処理装置署名鍵用マスター鍵 MK_{dev} とデータ処理装置識別子 ID_d

e v とに基づく暗号処理によりデータ処理装置固有鍵としての署名鍵 K d e v を生成するステップを含むことを特徴とする請求の範囲第 9 2 項に記載のデータ処理方法。

9 8. 上記署名鍵 K d e v 生成ステップは、

上記データ処理装置識別子 I D d e v に対して上記データ処理装置署名鍵用マスター鍵 M K d e v を適用した D E S 暗号処理により上記署名鍵 K d e v を生成するステップであることを特徴とする請求の範囲第 9 7 項に記載のデータ処理方法。

9 9. 上記データ処理方法は、さらに、

上記コンテンツデータに対する暗号処理を実行して中間チェック値を生成するステップを含み、

上記中間チェック値に上記データ処理装置固有鍵またはシステム共有鍵を適用した暗号処理を実行することを特徴とする請求の範囲第 9 2 項に記載のデータ処理方法。

1 0 0. 上記データ処理方法は、さらに、

上記コンテンツデータを複数部分に分割した部分データを 1 以上含む部分データ集合に対する暗号処理により部分チェック値を生成し、

該生成した部分チェック値を含む部分チェック値集合データ列に対する暗号処理により中間チェック値を生成することを特徴とする請求の範囲第 9 9 項に記載のデータ処理方法。

1 0 1. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラ

ムは、

上記コンテンツデータの利用態様に応じて、

上記コンテンツデータを利用する他のデータ処理装置に共通の暗号処理用システム共通鍵、または、データ処理装置固有の装置固有鍵のいずれかの暗号処理鍵を選択するステップと、

選択した暗号処理鍵を上記コンテンツデータに適用して暗号処理を実行するステップと、

を含むことを特徴とするプログラム提供媒体。

102. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理装置であり、

上記コンテンツデータに対する暗号処理を実行する暗号処理部と、

上記暗号処理部に対する制御を実行する制御部とを有し、

上記暗号処理部は、

データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位の正当性検証処理を実行する構成を有することを特徴とするデータ処理装置。

103. 上記データ処理装置は、コンテンツチェック値生成鍵を有し、

上記暗号処理部は、

検証対象のコンテンツブロックデータに基づいてコンテンツ中間値を生成し、該コンテンツ中間値に対する上記コンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成する構成であることを特徴とする請求の範囲第102項に記載のデータ処理装置。

104. 上記暗号処理部は、

検証対象のコンテンツブロックデータが暗号化されている場合、該コンテンツブロックデータの復号処理によって得られる復号文全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成し、

検証対象のコンテンツブロックデータが暗号化されていない場合、コンテンツブロックデータ全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成する構成であることを特徴とする請求の範囲第103項に記載のデータ処理装置。

105. 上記暗号処理部における上記中間チェック値の生成処理において適用する上記所定の演算処理は排他的論理和演算であることを特徴とする請求の範囲第104項に記載のデータ処理装置。

106. 上記暗号処理部は、

CBCモードによる暗号処理構成を有し、

検証対象のコンテンツブロックデータが暗号化されている場合のコンテンツ中間値生成処理に適用する上記復号処理は、CBCモードによる復号処理であることを特徴とする請求の範囲第104項に記載のデータ処理装置。

107. 上記暗号処理部の有するCBCモードによる暗号処理構成は、処理対象となるメッセージ列の一部においてのみ複数回数共通鍵暗号処理が適用される構成であることを特徴とする請求の範囲第106項に記載のデータ処理装置。

108. 上記暗号処理部は、

コンテンツブロックデータに複数のパーツが含まれ、該コンテンツブロックデータに含まれる一部のパーツが検証対象である場合において、検証対象パーツに基づいてコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位毎の

正当性検証処理を実行する構成を有することを特徴とする請求の範囲第102項に記載のデータ処理装置。

109. 上記暗号処理部は、

上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが1つである場合において、

上記要検証パーツが暗号化されている場合、要検証パーツの復号処理によって得られる復号文全体を所定バイト単位で排他論理和した値に、コンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成し、

上記要検証パーツが暗号化されていない場合、該要検証パーツ全体を所定バイト単位で排他論理和した値を、上記コンテンツチェック値生成鍵を適用して暗号処理を実行してコンテンツチェック値を生成する構成であることを特徴とする請求の範囲第108項に記載のデータ処理装置。

110. 上記暗号処理部は、

上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが複数である場合において、

各パーツ毎にコンテンツチェック値生成鍵を適用して暗号処理を実行して得られたパーツチェック値の連結データに対して、さらに上記コンテンツチェック値生成鍵を適用した暗号処理を実行して得られる結果をコンテンツチェック値とする構成であることを特徴とする請求の範囲第108項に記載のデータ処理装置。

111. 上記データ処理装置は、さらに、

上記暗号処理部において正当性検証の実行されたコンテンツブロックデータを含むコンテンツデータを格納する記録デバイスを有することを特徴とする請求の範囲第102項に記載のデータ処理装置。

1 1 2. 上記暗号処理部におけるコンテンツチェック値の照合処理において、照合が成立しなかった場合において、

上記制御部は、上記記録デバイスへの格納処理を中止する構成を有することを特徴とする請求の範囲第 1 1 1 項に記載のデータ処理装置。

1 1 3. 上記データ処理装置は、さらに、

上記暗号処理部において正当性検証の実行されたデータを再生する再生処理部を有することを特徴とする請求の範囲第 1 0 2 項に記載のデータ処理装置。

1 1 4. 上記データ処理装置は、

上記暗号処理部におけるコンテンツチェック値の照合処理において、照合が成立しなかった場合において、

上記制御部は、上記再生処理部での再生処理を中止する構成を有することを特徴とする請求の範囲第 1 1 3 項に記載のデータ処理装置。

1 1 5. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理方法であり、

データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成し、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位の正当性検証処理を実行することを特徴とするデータ処理方法。

1 1 6. 上記データ処理方法は、

検証対象のコンテンツブロックデータに基づいてコンテンツ中間値を生成し、生成したコンテンツ中間値に対するコンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成することを特徴とする請求の範囲第 1 1 5 項に記載のデータ処理方法。

1 1 7. 上記データ処理方法において、

検証対象のコンテンツブロックデータが暗号化されている場合、該コンテンツブロックデータの復号処理によって得られる復号文全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成し、

検証対象のコンテンツブロックデータが暗号化されていない場合、コンテンツブロックデータ全体を所定バイト単位で所定の演算処理を行いコンテンツ中間値を生成することを特徴とする請求の範囲第 1 1 5 項に記載のデータ処理方法。

1 1 8. 上記データ処理方法において、

上記中間チェック値の生成処理において適用する上記所定の演算処理は排他的論理和演算であることを特徴とする請求の範囲第 1 1 7 項に記載のデータ処理方法。

1 1 9. 上記コンテンツ中間値の生成処理において、

検証対象のコンテンツブロックデータが暗号化されている場合のコンテンツ中間値生成処理に適用する上記復号処理は、CBCモードによる復号処理であることを特徴とする請求の範囲第 1 1 7 項に記載のデータ処理方法。

1 2 0. 上記CBCモードによる復号処理構成は、処理対象となるメッセージ列の一部においてのみ複数回共通鍵暗号処理が適用することを特徴とする請求の範囲第 1 1 9 項に記載のデータ処理方法。

1 2 1. 上記データ処理方法において、

コンテンツブロックデータに複数のパーツが含まれ、該コンテンツブロックデータに含まれる一部のパーツが検証対象である場合、検証対象パーツに基づいてコンテンツチェック値を生成し、

生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位毎の正当性検証処理を実行することを特徴とする請求の範囲第115項に記載のデータ処理方法。

122. 上記データ処理方法において、

コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが1つである場合、

上記要検証パーツが暗号化されている場合、要検証パーツの復号処理によって得られる復号文全体を所定バイト単位で排他論理和した値に、コンテンツチェック値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成し、

上記要検証パーツが暗号化されていない場合、該要検証パーツ全体を所定バイト単位で排他論理和した値を、上記コンテンツチェック値生成鍵を適用して暗号処理を実行してコンテンツチェック値を生成することを特徴とする請求の範囲第121項に記載のデータ処理方法。

123. 上記データ処理方法において、

上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが複数である場合、

各パーツ毎にコンテンツチェック値生成鍵を適用して暗号処理を実行して得られたパーツチェック値の連結データに対して、さらに上記コンテンツチェック値生成鍵を適用した暗号処理を実行して得られる結果をコンテンツチェック値とすることを特徴とする請求の範囲第121項に記載のデータ処理方法。

124. 上記データ処理方法は、さらに、

正当性検証の実行されたコンテンツブロックデータを含むコンテンツデータを格納するステップを含むことを特徴とする請求の範囲第115項に記載のデータ処理方法。

1 2 5. 上記データ処理方法は、さらに、

コンテンツチェック値の照合処理において、照合が成立しなかった場合において、

上記制御部は、上記記録デバイスへの格納処理を中止することを特徴とする請求の範囲第 1 2 4 項に記載のデータ処理方法。

1 2 6. 上記データ処理方法は、さらに、

正当性検証の実行されたデータを再生する再生処理を実行するステップを含むことを特徴とする請求の範囲第 1 1 5 項に記載のデータ処理方法。

1 2 7. 上記データ処理方法は、

コンテンツチェック値の照合処理において、照合が成立しなかった場合において、再生処理を中止することを特徴とする請求の範囲第 1 2 6 項に記載のデータ処理方法。

1 2 8. コンテンツデータ検証処理のためのコンテンツデータ検証値付与方法であり、

データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成し、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とするコンテンツデータ検証値付与方法。

1 2 9. 上記コンテンツチェック値は、チェック対象となるコンテンツブロックデータをメッセージとし、コンテンツチェック値生成鍵を適用した暗号処理によって生成される値であることを特徴とする請求の範囲第 1 2 8 項に記載のコンテンツデータ検証値付与方法。

130. 上記コンテンツチェック値は、検証対象のコンテンツブロックデータに基づいてコンテンツ中間値を生成し、該コンテンツ中間値に対する上記コンテンツチェック値生成鍵を適用した暗号処理を実行して生成される値であることを特徴とする請求の範囲第128項に記載のコンテンツデータ検証値付与方法。

131. 上記コンテンツチェック値は、検証対象のコンテンツブロックデータに対するCBCモードによる暗号処理を実行することによって生成される値であることを特徴とする請求の範囲第128項に記載のコンテンツデータ検証値付与方法。

132. 上記CBCモードによる暗号処理構成は、処理対象となるメッセージ列の一部においてのみ複数回共通鍵暗号処理が適用される構成であることを特徴とする請求の範囲第131項に記載のコンテンツデータ検証値付与方法。

133. 上記コンテンツデータ検証値付与方法において、

コンテンツブロックデータに複数のパーツが含まれ、該コンテンツブロックデータに含まれる一部のパーツを検証対象とする場合において、検証対象パーツに基づいてコンテンツチェック値を生成し、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とする請求の範囲第128項に記載のコンテンツデータ検証値付与方法。

134. 上記コンテンツデータ検証値付与方法において、

上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが1つである場合において、

上記要検証パーツが暗号化されている場合、要検証パーツの復号処理によって得られる復号文全体を所定バイト単位で排他論理和した値に、コンテンツチェッ

ク値生成鍵を適用した暗号処理を実行してコンテンツチェック値を生成し、

上記要検証パーツが暗号化されていない場合、該要検証パーツ全体を所定バイト単位で排他論理和した値を、上記コンテンツチェック値生成鍵を適用して暗号処理を実行してコンテンツチェック値を生成し、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とする請求の範囲第133項に記載のコンテンツデータ検証値付与方法。

135. 上記コンテンツデータ検証値付与方法において、

上記コンテンツブロックデータに複数のパーツが含まれ、検証対象である要検証パーツが複数である場合において、

各パーツ毎にコンテンツチェック値生成鍵を適用して暗号処理を実行して得られたパーツチェック値の連結データに対して、さらに上記コンテンツチェック値生成鍵を適用した暗号処理を実行して得られる結果をコンテンツチェック値とし、生成したコンテンツチェック値を検証対象コンテンツブロックデータを含むコンテンツデータに付与することを特徴とする請求の範囲第133項に記載のコンテンツデータ検証値付与方法。

136. 記憶媒体または通信媒体によって提供されるコンテンツデータの処理を行なうデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、

データに含まれる検証対象のコンテンツブロックデータ単位にコンテンツチェック値を生成するステップと、生成したコンテンツチェック値の照合処理を実行することにより、上記データ中のコンテンツブロックデータ単位の正当性検証処理を実行するステップと、

を含むことを特徴とするプログラム提供媒体。

137. 少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データを生成する処理を実行するデータ処理装置であり、

上記データ処理装置は、

上記記録デバイスに対する格納対象となるコンテンツデータが、上記コンテンツブロックの暗号鍵 K_{con} を暗号鍵 K_{dis} によって暗号処理した暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部に格納したデータによって構成されている場合において、

上記暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部から取り出して復号処理を実行して復号データ K_{con} を生成し、該生成した復号データ K_{con} に対して異なる暗号鍵 K_{str} を適用して暗号処理を実行することにより、暗号鍵 K_{str} によって暗号処理された新たな暗号鍵データ $K_{str}[K_{con}]$ を生成して上記コンテンツデータのヘッダ部に格納する処理を実行する構成を有することを特徴とするデータ処理装置。

138. 少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データを生成する処理を実行するデータ処理装置であり、

上記データ処理装置は、

上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵 K_{blc} によって暗号化されたコンテンツと、暗号鍵 K_{con} によって暗号化された暗号鍵データ $K_{con}[K_{blc}]$ によって構成され、さらに、暗号鍵 K_{con} を暗号鍵 K_{dis} によって暗号処理した暗号鍵データ $K_{dis}[K_{con}]$ を上記ヘッダ部に格納した構成を有する場合において、

上記暗号鍵データ $Kdis[Kcon]$ を上記ヘッダ部から取り出して復号処理を実行して復号データ $Kcon$ を生成し、該生成した復号データ $Kcon$ に対して異なる暗号鍵 $Kstr$ を適用して暗号処理を実行することにより、暗号鍵 $Kstr$ によって暗号処理された暗号鍵データ $Kstr[Kcon]$ を生成して上記コンテンツデータのヘッダ部に格納する処理を実行する構成を有することを特徴とするデータ処理装置。

139. 少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データを生成する処理を実行するデータ処理装置であり、

上記データ処理装置は、

上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵 $Kblc$ によって暗号化されたコンテンツと、暗号鍵 $Kdis$ によって暗号化された暗号鍵データ $Kdis[Kblc]$ によって構成されている場合において、

上記暗号鍵データ $Kdis[Kblc]$ を上記コンテンツブロック部から取り出して、該暗号鍵 $Kblc$ の復号処理を実行して復号データ $Kblc$ を生成し、該生成した復号データ $Kblc$ に対して異なる暗号鍵 $Kstr$ を適用して暗号処理を実行することにより、暗号鍵 $Kstr$ によって暗号処理された暗号鍵 $Kstr[Kblc]$ を生成してコンテンツブロック部に格納する処理を実行する構成を有することを特徴とするデータ処理装置。

140. コンテンツデータを生成するコンテンツデータ生成方法であり、

音声情報、画像情報、プログラムデータの少なくともいずれかを含むデータによって構成されるコンテンツブロックを複数ブロック連結し、

複数のコンテンツブロックに含まれる少なくとも一部のコンテンツブロックを

暗号鍵K c o nによって暗号処理し、

上記暗号鍵K c o nを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K c o n] を生成して上記コンテンツデータのヘッダ部に格納し、
複数のコンテンツブロックとヘッダ部を含むコンテンツデータを生成するコンテンツデータ生成方法。

1 4 1. 上記コンテンツデータ生成方法は、さらに、

コンテンツデータの識別情報、

コンテンツデータのデータ長、コンテンツデータのデータ種類を含む取扱方針情報、

上記コンテンツブロックのデータ長、暗号処理の有無を含む情報を格納したブロック情報を生成して、上記ヘッダ部に格納する処理を含むことを特徴とする請求の範囲第1 4 0項に記載のコンテンツデータ生成方法。

1 4 2. 上記コンテンツデータ生成方法は、さらに、

上記ヘッダ部を構成する一部の情報に基づく部分チェック値を生成して、該部分チェック値を上記ヘッダ部に格納し、

さらに、上記部分チェック値に基づく総チェック値を生成して、該総チェック値を上記ヘッダ部に格納する処理を含むことを特徴とする請求の範囲第1 4 0項に記載のコンテンツデータ生成方法。

1 4 3. 上記部分チェック値の生成処理および総チェック値の生成処理は、

チェック対象となるデータをメッセージとし、チェック値生成鍵を暗号鍵とするDES暗号処理アルゴリズムを適用して実行することを特徴とする請求の範囲第1 4 2項に記載のコンテンツデータ生成方法。

1 4 4. 上記コンテンツデータ生成方法は、さらに、

上記ブロック情報を暗号鍵K b i tにより暗号化处理し、該暗号鍵K b i tを暗号鍵K d i sによって生成した暗号鍵データK d i s [K b i t]を上記ヘッダ部に格納することを特徴とする請求の範囲第1 4 1項に記載のコンテンツデータ生成方法。

1 4 5. 上記コンテンツブロック中の複数ブロックの各々のブロックは共通する一定のデータ長として生成することを特徴とする請求の範囲第1 4 0項に記載のコンテンツデータ生成方法。

1 4 6. 上記コンテンツブロック中の複数ブロックの各々のブロックは暗号データ部と非暗号データ部とを規則的に配列した構成として生成することを特徴とする請求の範囲第1 4 0項に記載のコンテンツデータ生成方法。

1 4 7. コンテンツデータを生成するコンテンツデータ生成方法であり、

音声情報、画像情報、プログラムデータの少なくともいずれかを含むコンテンツブロックを複数ブロック連結するとともに、

複数のコンテンツブロックの少なくとも一部のブロックを、音声情報、画像情報、プログラムデータの少なくともいずれかを含むデータを暗号鍵K b l cで暗号化した暗号データ部と、該暗号データ部の暗号鍵K b l cを暗号鍵K c o nによって暗号処理した暗号鍵データK c o n [K b l c]の組によって構成し、

上記暗号鍵K c o nを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K c o n]を生成して上記コンテンツデータのヘッダ部に格納し、

複数のコンテンツブロックとヘッダ部を含むコンテンツデータを生成するコンテンツデータ生成方法。

1 4 8. コンテンツデータを生成するコンテンツデータ生成方法であり、

音声情報、画像情報、プログラムデータの少なくともいずれかを含むコンテン

ツブロックを複数ブロック連結するとともに、

複数のコンテンツブロックの少なくとも一部のブロックを、音声情報、画像情報、プログラムデータの少なくともいずれかを含むデータを暗号鍵K b l cで暗号化した暗号データ部と、該暗号データ部の暗号鍵K b l cを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K b l c]の組によって構成し、

複数のコンテンツブロックとヘッダ部を含むコンテンツデータを生成するコンテンツデータ生成方法。

149. 少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納処理を実行するデータ処理方法であり、

上記記録デバイスに対する格納対象となるコンテンツデータが、上記コンテンツブロックの暗号鍵K c o nを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K c o n]を上記ヘッダ部に格納したデータによって構成されている場合において、

上記暗号鍵データK d i s [K c o n]を上記ヘッダ部から取り出して復号処理を実行して復号データK c o nを生成し、

該生成した復号データK c o nに対して異なる暗号鍵K s t rを適用して暗号処理を実行することにより、暗号鍵K s t rによって暗号処理された新たな暗号鍵データK s t r [K c o n]を生成し、

上記生成した暗号鍵データK s t r [K c o n]を上記コンテンツデータのヘッダ部に格納し、上記複数のコンテンツブロックと共に上記記録デバイスに格納することを特徴とするデータ処理方法。

150. 少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納処理を実行するデータ処理方法であり、

上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵K b l cによって暗号化されたコンテンツと、暗号鍵K c o nによって暗号化された暗号鍵データK c o n [K b l c]によって構成され、さらに、暗号鍵K c o nを暗号鍵K d i sによって暗号処理した暗号鍵データK d i s [K c o n]を上記ヘッダ部に格納した構成を有する場合において、

上記暗号鍵データK d i s [K c o n]を上記ヘッダ部から取り出して復号処理を実行して復号データK c o nを生成し、

該生成した復号データK c o nに対して異なる暗号鍵K s t rを適用して暗号処理を実行することにより、暗号鍵K s t rによって暗号処理された暗号鍵データK s t r [K c o n]を生成し、

上記生成した暗号鍵データK s t r [K c o n]を上記コンテンツデータのヘッダ部に格納し、上記複数のコンテンツブロックと共に上記記録デバイスに格納することを特徴とするデータ処理方法。

151. 少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納処理を実行するデータ処理方法であり、

上記記録デバイスに対する格納対象となるコンテンツデータに含まれる上記コンテンツブロックが、暗号鍵K b l cによって暗号化されたコンテンツと、暗号鍵K d i sによって暗号化された暗号鍵データK d i s [K b l c]によって構成されている場合において、

上記暗号鍵データK d i s [K b l c]を上記コンテンツブロック部から取り出して、該暗号鍵K b l cの復号処理を実行して復号データK b l cを生成し、

該生成した復号データK b l cに対して異なる暗号鍵K s t rを適用して暗号処理を実行することにより、暗号鍵K s t rによって暗号処理された暗号鍵K s t r [K b l c]を生成し、

該生成した暗号鍵 $K_{str} [K_{blc}]$ をコンテンツブロック部に格納し、複数のコンテンツブロックと共に上記記録デバイスに格納することを特徴とするデータ処理方法。

152. 少なくとも一部のブロックが暗号化された複数のコンテンツブロックと、該コンテンツブロックに関する情報を格納したヘッダ部を有するコンテンツデータの記録デバイスに対する格納データの生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、

上記記録デバイスに対する格納対象となるコンテンツデータが、上記コンテンツブロックの暗号鍵 K_{con} を暗号鍵 K_{dis} によって暗号処理した暗号鍵データ $K_{dis} [K_{con}]$ を上記ヘッダ部に格納したデータによって構成されている場合において、

上記暗号鍵データ $K_{dis} [K_{con}]$ を上記ヘッダ部から取り出して復号処理を実行して復号データ K_{con} を生成するステップと、

該生成した復号データ K_{con} に対して異なる暗号鍵 K_{str} を適用して暗号処理を実行することにより、暗号鍵 K_{str} によって暗号処理された新たな暗号鍵データ $K_{str} [K_{con}]$ を生成するステップと、

上記生成した暗号鍵データ $K_{str} [K_{con}]$ を上記コンテンツデータのヘッダ部に格納するステップと、

を含むことを特徴とするプログラム提供媒体。

153. 記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理を行なうデータ処理装置であり、

圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを含むコンテンツデータのコンテンツデータ解析を実行し、該コンテンツデータから圧縮コンテンツと、伸長処理プログラムの抽出処理を実行するコンテンツデータ解析部

と、

上記コンテンツデータ解析部の解析結果として得られたコンテンツデータに含まれる伸長処理プログラムを用いて該コンテンツデータに含まれる圧縮コンテンツの伸長処理を実行する伸長処理部と、

を有することを特徴とするデータ処理装置。

154. 上記データ処理装置は、さらに、

上記コンテンツデータ解析部によって抽出された圧縮コンテンツを格納するデータ記憶部と、

上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶部とを有し、

上記伸長処理部は、

上記データ記憶部に記憶された圧縮コンテンツに対して、上記プログラム記憶部に記憶された伸長処理プログラムを適用して伸長処理を実行する構成を有することを特徴とする請求の範囲第153項に記載のデータ処理装置。

155. 上記コンテンツデータ解析部は、

上記コンテンツデータに含まれるヘッダ情報に基づいてコンテンツデータの構成情報を取得してコンテンツデータの解析を行なう構成であることを特徴とする請求の範囲第153項に記載のデータ処理装置。

156. 上記ヘッダ情報には、

圧縮コンテンツの再生優先順位情報が含まれ、

上記伸長処理部において伸長処理対象となる圧縮コンテンツが複数ある場合、

上記伸長処理部は、

上記コンテンツデータ解析部において取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次コンテンツ伸長処理を実行する構成である

ことを特徴とする請求の範囲第155項に記載のデータ処理装置。

157. 上記データ処理装置は、さらに、

伸長処理対象となる圧縮コンテンツの情報を表示する表示手段と、

上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力手段を有し、

上記伸長処理部は、

上記入力手段から入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行する構成であることを特徴とする請求の範囲第153項に記載のデータ処理装置。

158. 記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理を行なうデータ処理装置であり、

圧縮コンテンツ、または伸長処理プログラムのいずれかを含むコンテンツデータを受領し、受領コンテンツデータに含まれるヘッダ情報から該コンテンツデータが圧縮コンテンツであるか伸長処理プログラムであるかを判別するとともに、

該コンテンツデータが圧縮コンテンツである場合、該コンテンツデータのヘッダ情報から、該圧縮コンテンツに適用された圧縮処理プログラム種類を取得し、

該コンテンツデータが伸長処理プログラムである場合、該コンテンツデータのヘッダ情報から伸長処理プログラム種類を取得するコンテンツデータ解析部と、

圧縮コンテンツの伸長処理を実行する伸長処理部とを有し、

上記伸長処理部は、

上記コンテンツデータ解析部が解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、上記コンテンツデータ解析部によって解析された伸長処理プログラム種類に基づいて選択し、該選択した伸長処理プログラムによる伸長処理を実行する構成を有することを特徴とするデータ処理装置。

159. 上記データ処理装置は、さらに、

上記コンテンツデータ解析部によって抽出された圧縮コンテンツを格納するデータ記憶部と、

上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶部とを有し、

上記伸長処理部は、

上記データ記憶部に記憶された圧縮コンテンツに対して、上記プログラム記憶部に記憶された伸長処理プログラムを適用して伸長処理を実行する構成を有することを特徴とする請求の範囲第158項に記載のデータ処理装置。

160. 上記ヘッダ情報には、

圧縮コンテンツの再生優先順位情報が含まれ、伸長処理対象となる圧縮コンテンツが複数ある場合、

上記伸長処理部におけるコンテンツ伸長処理は、

上記コンテンツデータ解析部において取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次実行する構成であることを特徴とする請求の範囲第158項に記載のデータ処理装置。

161. 上記データ処理装置は、

伸長処理プログラムを検索する検索手段を有し、

上記検索手段は、

上記コンテンツデータ解析部が解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、上記データ処理装置がアクセス可能なプログラム格納手段を検索対象として検索する構成であることを特徴とする請求の範囲第158項に記載のデータ処理装置。

1 6 2. 上記データ処理装置は、さらに、

伸長処理対象となる圧縮コンテンツの情報を表示する表示手段と、

上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力手段を有し、

上記伸長処理部は、

上記入力手段から入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行する構成であることを特徴とする請求の範囲第 1 5 8 項に記載のデータ処理装置。

1 6 3. 記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理を行なうデータ処理方法であり、

圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを含むコンテンツデータのコンテンツデータ解析を実行し、該コンテンツデータから圧縮コンテンツと、伸長処理プログラムの抽出処理を実行するコンテンツデータ解析ステップと、

上記コンテンツデータ解析ステップの解析結果として得られたコンテンツデータに含まれる伸長処理プログラムを用いて該コンテンツデータに含まれる圧縮コンテンツの伸長処理を実行する伸長処理ステップと、

を有することを特徴とするデータ処理方法。

1 6 4. 上記データ処理方法は、さらに、

上記コンテンツデータ解析ステップによって抽出された圧縮コンテンツを格納するデータ記憶ステップと、

上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶ステップとを有し、

上記伸長処理ステップは、

上記データ記憶ステップにおいて記憶された圧縮コンテンツに対して、上記プ

ログラム記憶ステップにおいて記憶された伸長処理プログラムを適用して伸長処理を実行する構成を有することを特徴とする請求の範囲第163項に記載のデータ処理方法。

165. 上記コンテンツデータ解析ステップは、

上記コンテンツデータに含まれるヘッダ情報に基づいてコンテンツデータの構成情報を取得してコンテンツデータの解析を行なうことを特徴とする請求の範囲第163項に記載のデータ処理方法。

166. 上記ヘッダ情報には、

圧縮コンテンツの再生優先順位情報が含まれ、

上記伸長処理部において伸長処理対象となる圧縮コンテンツが複数ある場合、上記伸長処理ステップは、

上記コンテンツデータ解析ステップにおいて取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次コンテンツ伸長処理を実行することを特徴とする請求の範囲第165項に記載のデータ処理方法。

167. 上記データ処理方法は、さらに、

伸長処理対象となる圧縮コンテンツの情報を表示手段に表示する表示ステップと、

上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力ステップとを有し、

上記伸長処理ステップは、

上記入力ステップにおいて入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行することを特徴とする請求の範囲第163項に記載のデータ処理方法。

168. 記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理を行なうデータ処理方法であり、

圧縮コンテンツ、または伸長処理プログラムのいずれかを含むコンテンツデータを受領し、受領コンテンツデータに含まれるヘッダ情報から該コンテンツデータが圧縮コンテンツであるか伸長処理プログラムであるかを判別するとともに、

該コンテンツデータが圧縮コンテンツである場合、該コンテンツデータのヘッダ情報から、該圧縮コンテンツに適用された圧縮処理プログラム種類を取得し、

該コンテンツデータが伸長処理プログラムである場合、該コンテンツデータのヘッダ情報から伸長処理プログラム種類を取得するコンテンツデータ解析ステップと、

上記コンテンツデータ解析ステップにおいて解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、上記コンテンツデータ解析ステップによって解析された伸長処理プログラム種類に基づいて選択する選択ステップと、

上記選択ステップにおいて選択した伸長処理プログラムによる伸長処理を実行する伸長処理ステップと、

を有することを特徴とするデータ処理方法。

169. 上記データ処理方法は、さらに、

上記コンテンツデータ解析部によって抽出された圧縮コンテンツを格納するデータ記憶ステップと、

上記コンテンツデータ解析部によって抽出された伸長処理プログラムを格納するプログラム記憶ステップとを有し、

上記伸長処理ステップは、

上記データ記憶ステップにおいて記憶された圧縮コンテンツに対して、上記プログラム記憶ステップにおいて記憶された伸長処理プログラムを適用して伸長処理を実行することを特徴とする請求の範囲第168項に記載のデータ処理方法。

170. 上記ヘッダ情報には、

圧縮コンテンツの再生優先順位情報が含まれ、伸長処理対象となる圧縮コンテンツが複数ある場合、

上記伸長処理ステップは、

上記コンテンツデータ解析ステップにおいて取得されたヘッダ情報中の優先順位情報に基づいて、該優先順位に従って順次実行することを特徴とする請求の範囲第168項に記載のデータ処理方法。

171. 上記データ処理方法は、さらに、

伸長処理プログラムを検索する検索ステップを有し、

上記検索ステップは、

上記コンテンツデータ解析ステップにおいて解析した圧縮コンテンツの圧縮処理プログラム種類に対して適用可能な伸長処理プログラムを、アクセス可能なプログラム格納手段を検索対象として検索することを特徴とする請求の範囲第168項に記載のデータ処理方法。

172. 上記データ処理方法は、さらに、

伸長処理対象となる圧縮コンテンツの情報を表示手段に表示する表示ステップと、

上記表示手段に表示されたコンテンツ情報から選択された再生コンテンツ識別データを入力する入力ステップとを有し、

上記伸長処理ステップは、

上記入力手段から入力された再生コンテンツ識別データに基づいて、該識別データに対応する圧縮コンテンツの伸長処理を実行することを特徴とする請求の範囲第168項に記載のデータ処理方法。

173. 記憶媒体または通信媒体によって提供するコンテンツデータの生成処理を行なうコンテンツデータ生成方法であり、

圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを組み合わせたコンテンツデータを生成することを特徴とするコンテンツデータ生成方法。

174. 上記コンテンツデータ生成方法において、さらに、

上記コンテンツデータのヘッダ情報として該コンテンツデータの構成情報を付加することを特徴とする請求の範囲第173項に記載のコンテンツデータ生成方法。

175. 上記コンテンツデータ生成方法において、さらに、

上記コンテンツデータのヘッダ情報として、該コンテンツデータに含まれるコンテンツの再生優先順位情報を付加することを特徴とする請求の範囲第173項に記載のコンテンツデータ生成方法。

176. 記憶媒体または通信媒体によって提供されるコンテンツデータの生成処理を行なうコンテンツデータ生成方法であり、

コンテンツデータが圧縮コンテンツであるか伸長処理プログラムであるかを識別するコンテンツデータ種類をヘッダ情報として付加し、

該コンテンツデータが圧縮コンテンツである場合は、該圧縮コンテンツに適用された圧縮処理プログラム種類をヘッダ情報として付加し、

該コンテンツデータが伸長処理プログラムである場合は、伸長処理プログラム種類をヘッダ情報として付加したコンテンツデータを生成することを特徴とするコンテンツデータ生成方法。

177. 上記コンテンツデータ生成方法において、さらに、

上記コンテンツデータのヘッダ情報として、該コンテンツデータに含まれるコ

ンテンツの再生優先順位情報を付加することを特徴とする請求の範囲第 1 7 6 項に記載のコンテンツデータ生成方法。

1 7 8. 記憶媒体または通信媒体によって提供されるコンテンツデータの再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、上記コンピュータ・プログラムは、

圧縮されたコンテンツと該圧縮コンテンツの伸長処理プログラムとを含むコンテンツデータのコンテンツデータ解析を実行し、該コンテンツデータから圧縮コンテンツと、伸長処理プログラムの抽出処理を実行するコンテンツデータ解析ステップと、

上記コンテンツデータ解析ステップの解析結果として得られたコンテンツデータに含まれる伸長処理プログラムを用いて該コンテンツデータに含まれる圧縮コンテンツの伸長処理を実行する伸長処理ステップと、

を有することを特徴とするプログラム提供媒体。

THIS PAGE BLANK (user to)

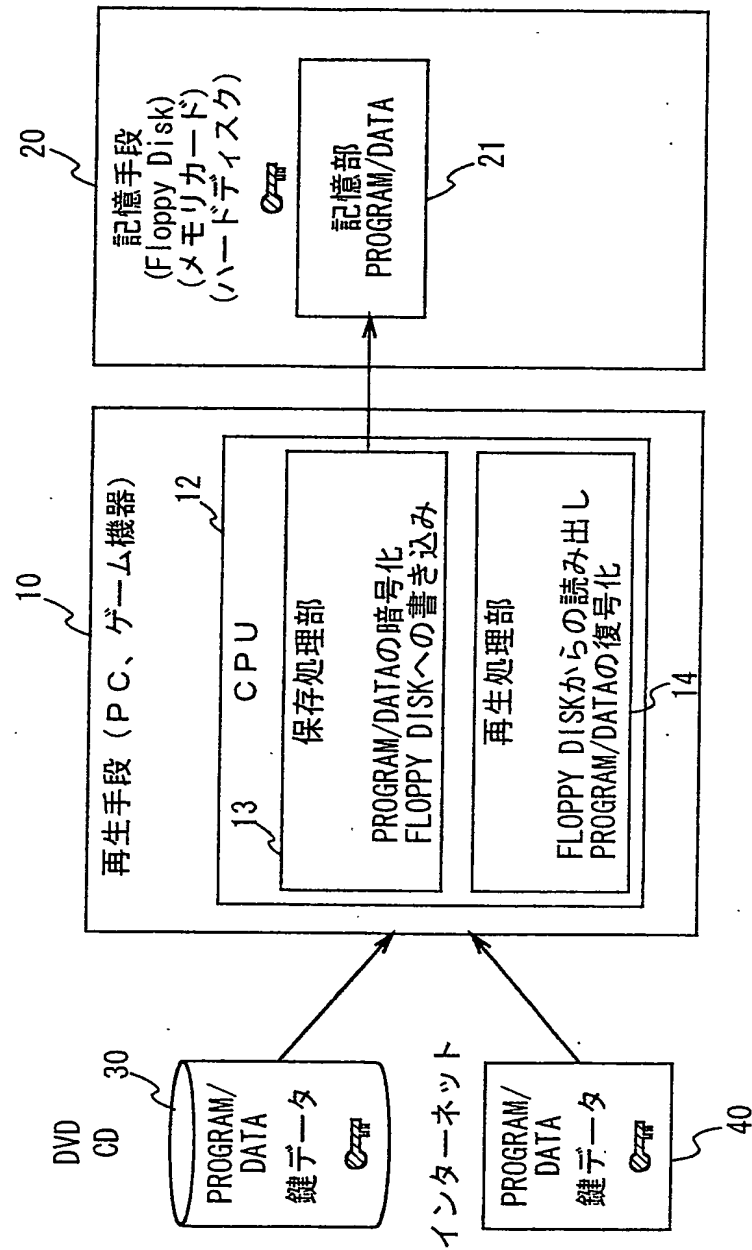


図 1

THIS PAGE BLANK (uspro)

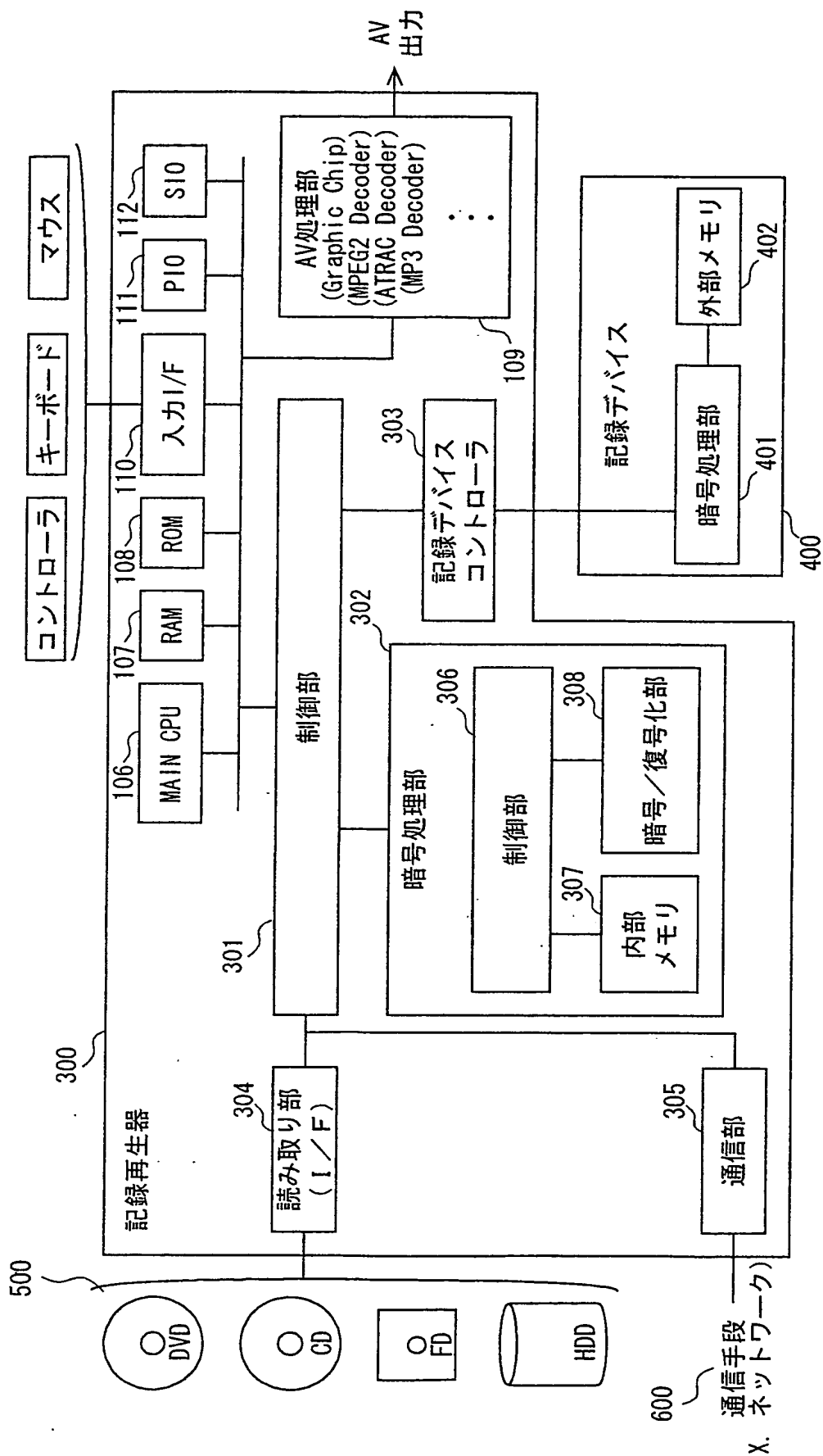


図 2

THIS PAGE BLANK (uspto)

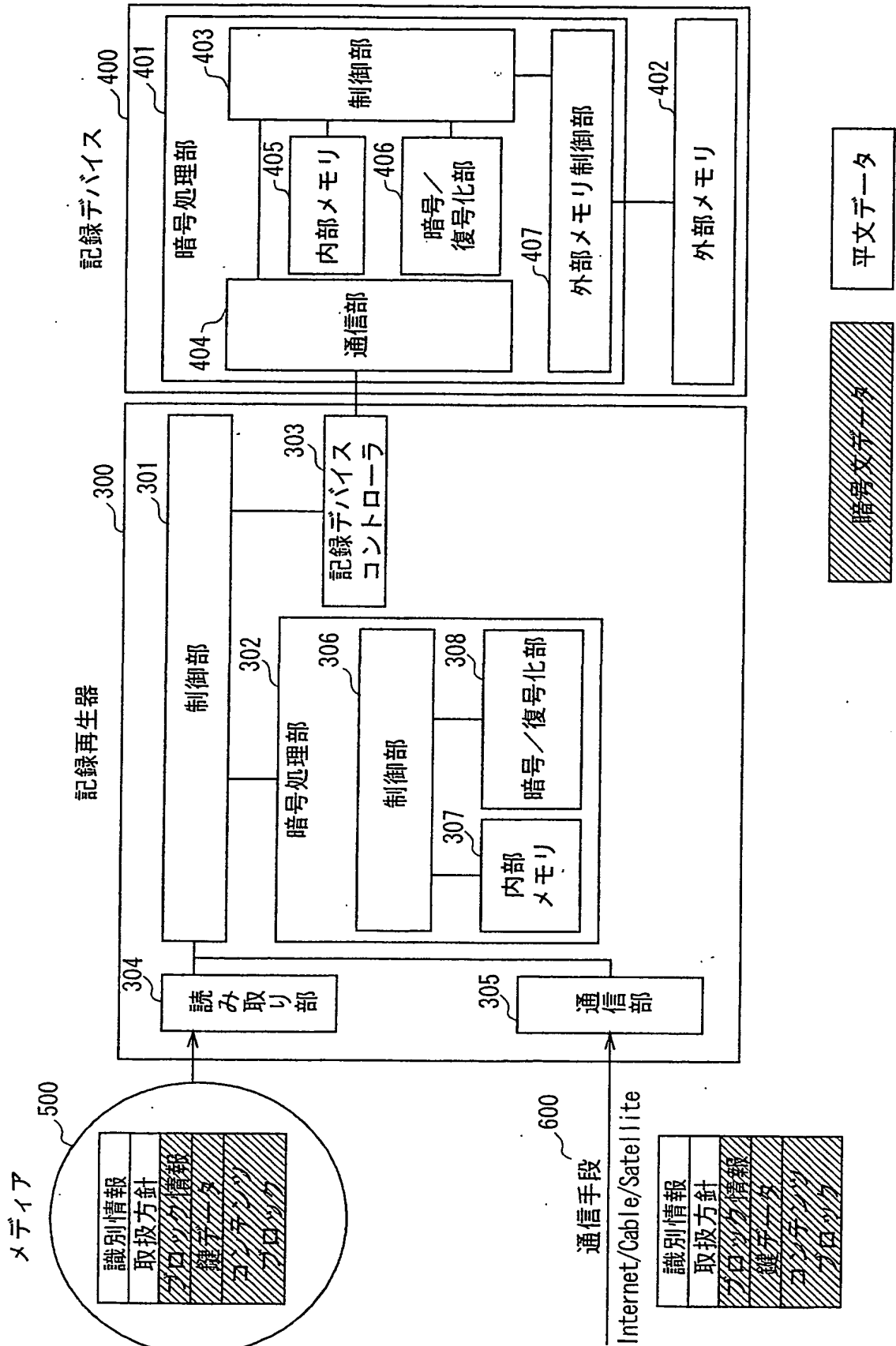
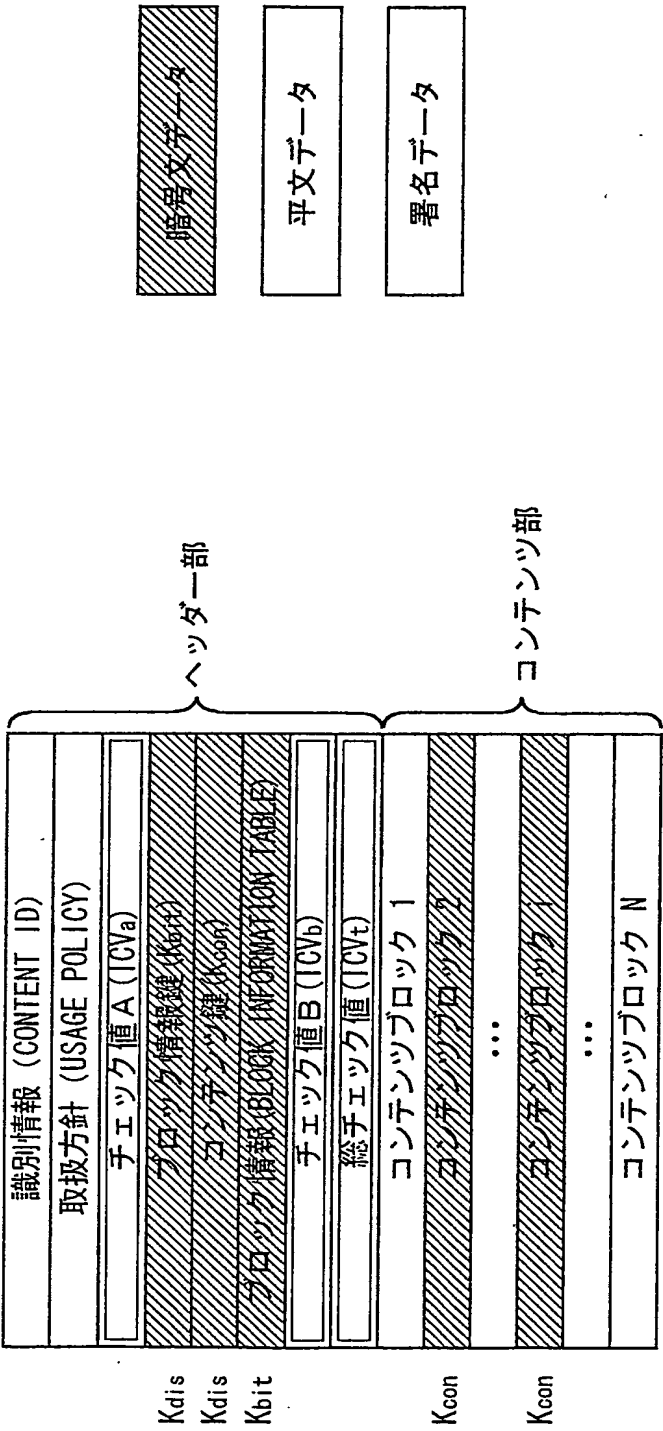


図3

THIS PAGE BLANK (USPTO)



メディア上及び通信路上のデータフォーマット

図 4

THIS SIDE
PAGE BLANK (USPTO)

ヘッダーサイズ (Header Length)
コンテンツサイズ (Content Length)
フォーマットバージョン (Format Version)
フォーマットタイプ (Format Type)
コンテンツタイプ (Content Type)
起動優先順位情報 (Operation Priority)
利用制限情報 (Localization Field)
複製制限情報 (Copy Permission)
移動制限情報 (Move Permission)
暗号アルゴリズム (Encryption Algorithm)
暗号化モード (Encryption Mode)
検証方法 (Integrity Check Method)

取扱方針

図 5

THIS PAGE BLANK (uspto)

Kbit

コンテンツブロック数 (Block Number)	
ブ ロ ッ ク 1	ブロックサイズ (Block Length)
	暗号化フラグ (Encryption Flag)
	検証対象フラグ (ICV Flag)
	コンテンツチェック値 (ICV1)
.	
.	
.	
.	
ブ ロ ッ ク N	ブロックサイズ (Block Length)
	暗号化フラグ (Encryption Flag)
	検証対象フラグ (ICV Flag)
	コンテンツチェック値 (ICVN)

ブロック情報

図 6

THIS PAGE BLANK (uspto)

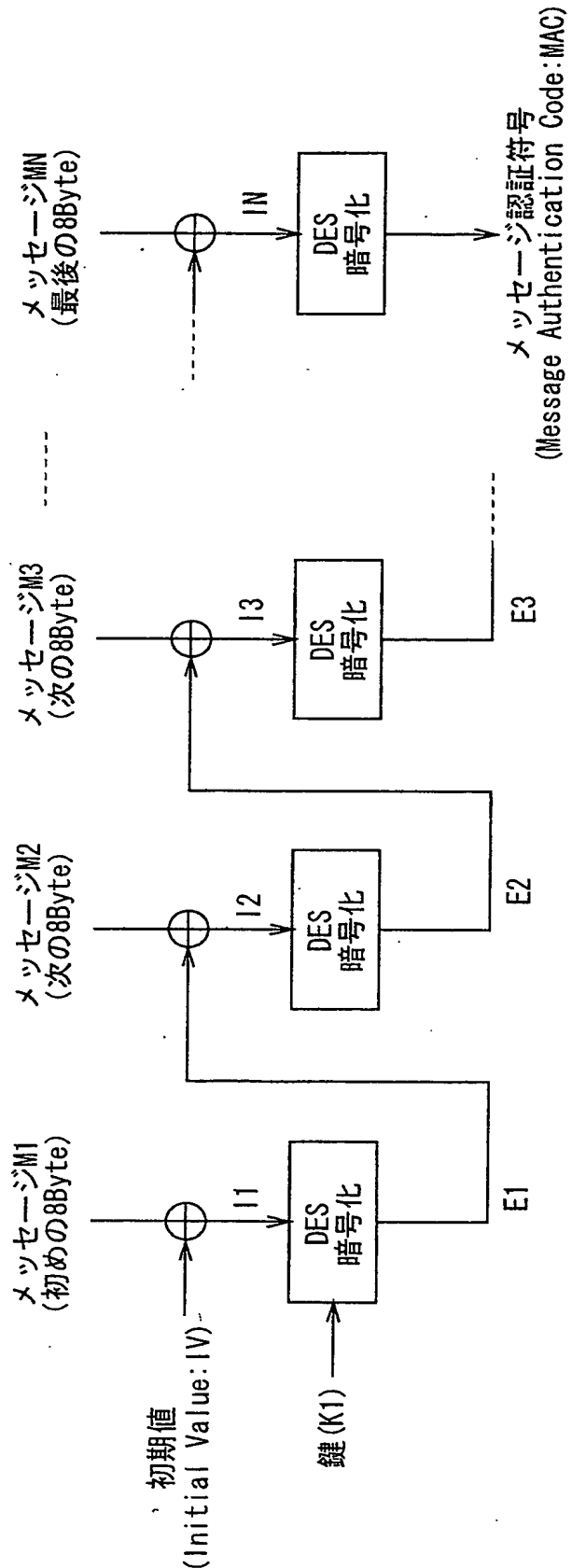


図 7

⊕: 排他的論理和処理 (8バイト単位)

THIS PAGE BLANK (uspto)

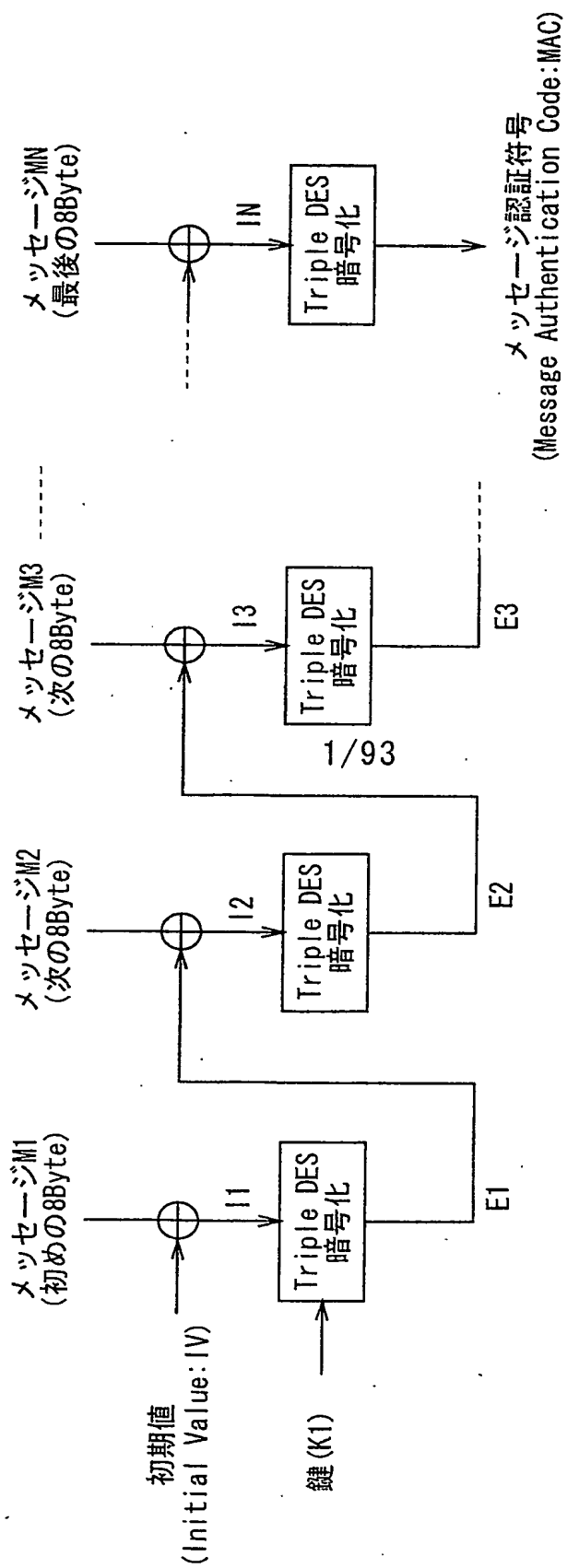


図 8

THIS PAGE BLANK (USPTO)
THIS PAGE BLANK (USPTO)

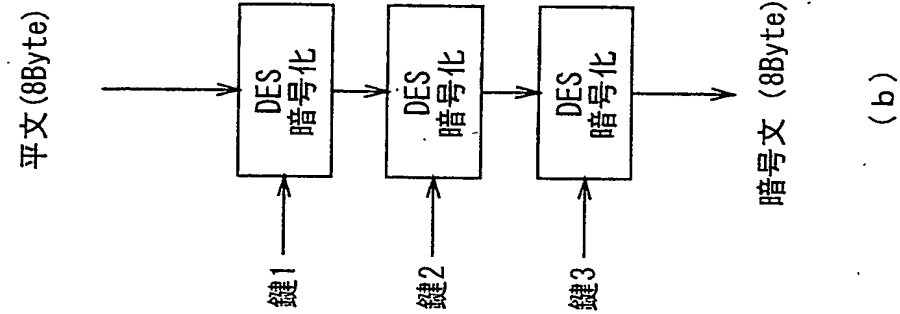
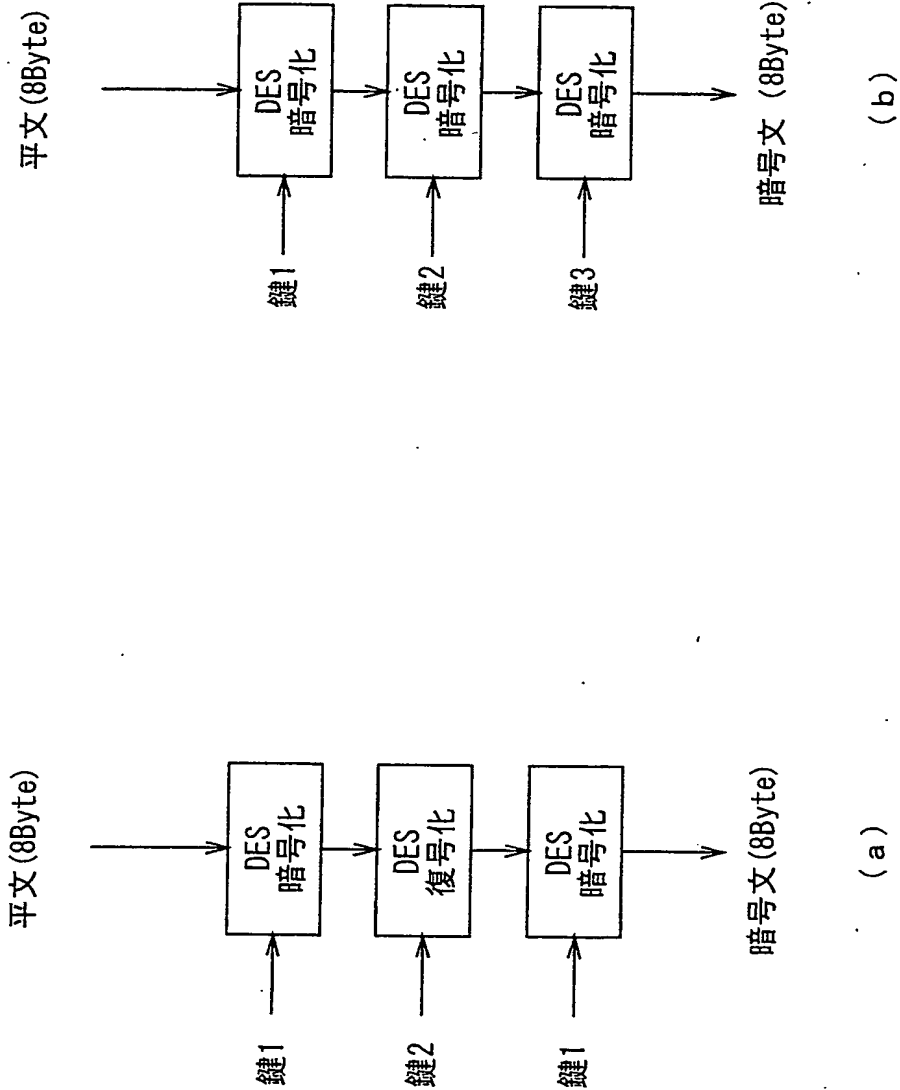


図 9

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

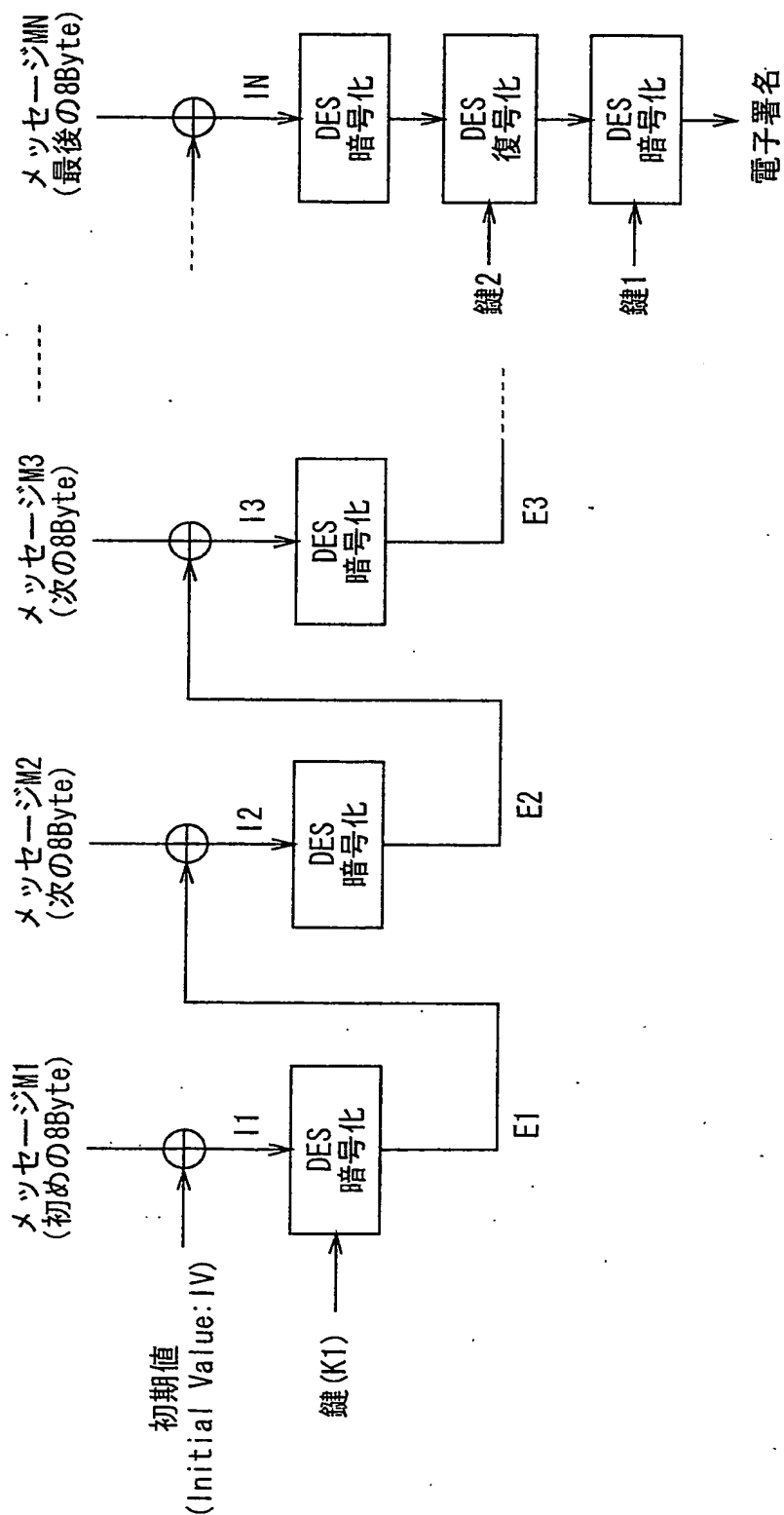
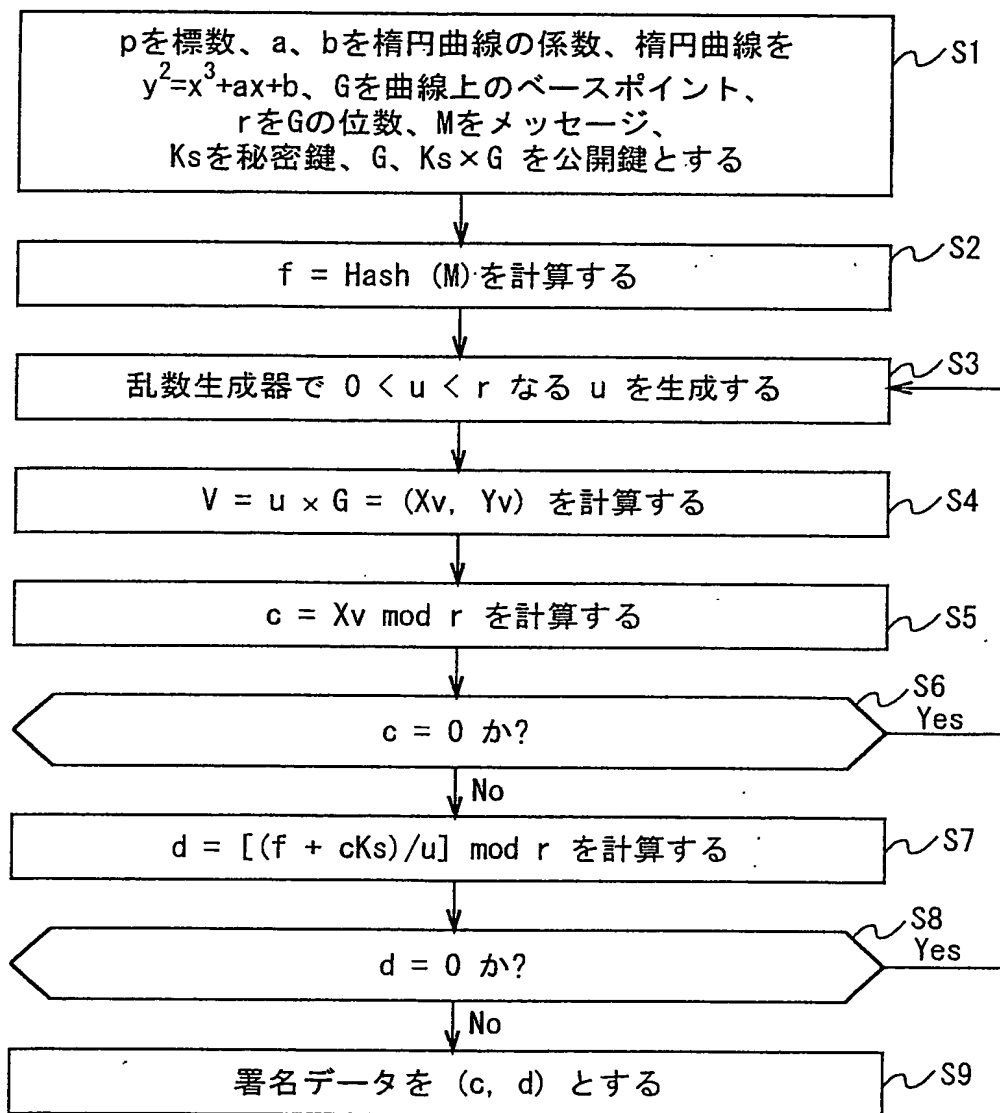
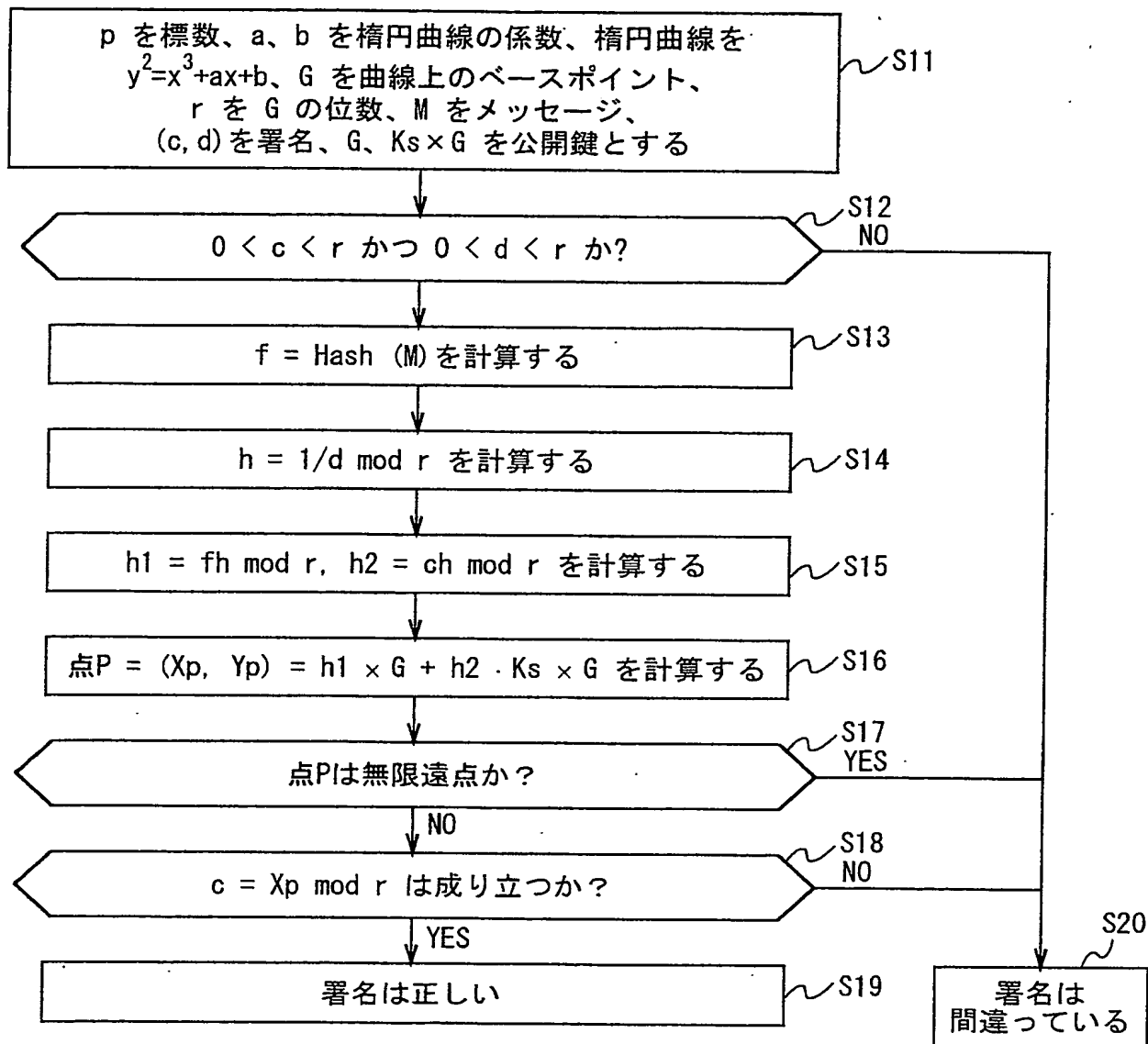


図 10

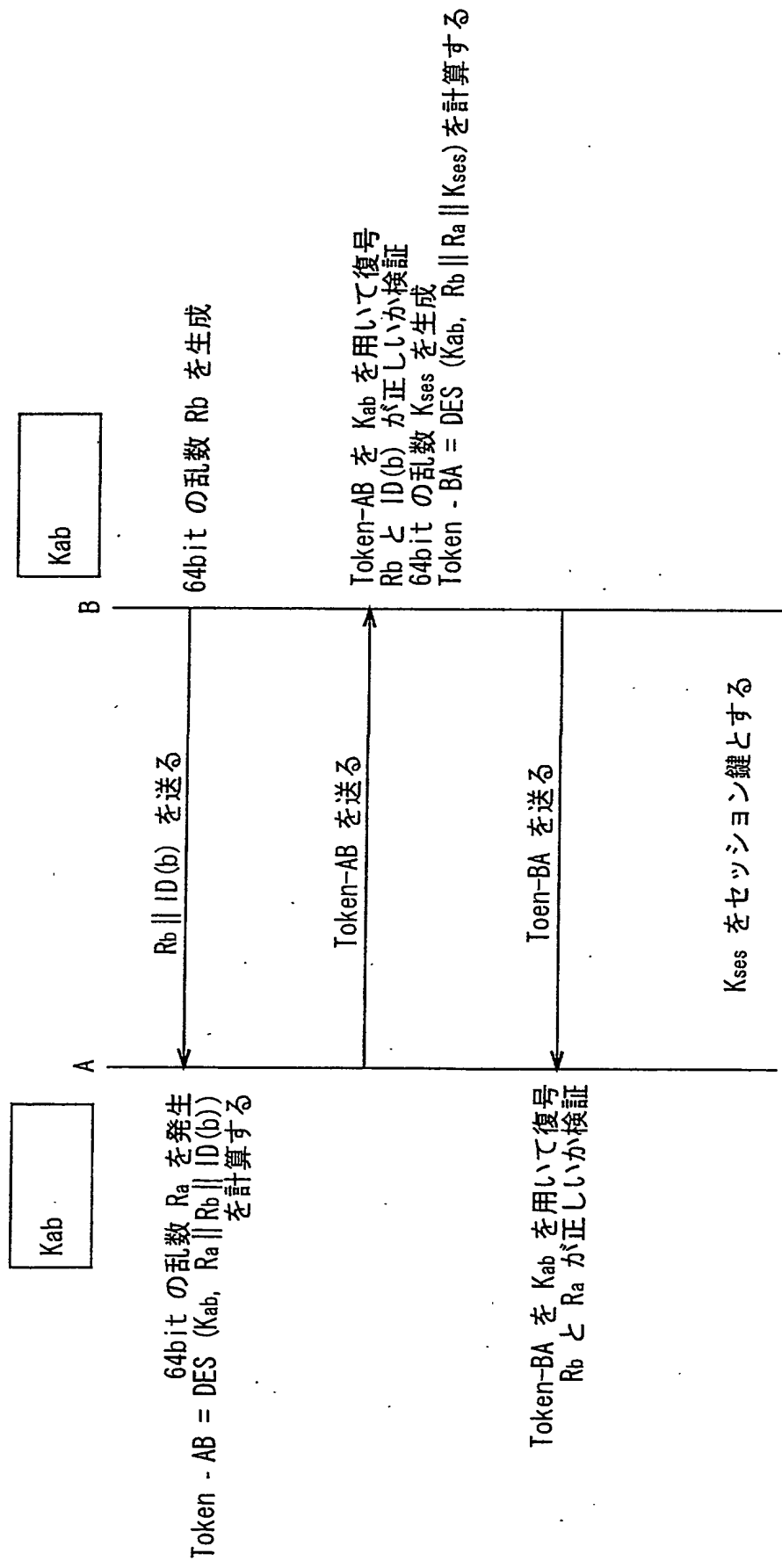
THIS PAGE BLANK (USPTO)

署名生成署名生成 (IEEE P1363/D3)

THIS PAGE BLANK (USPTO)

署名検証署名検証 (IEEE P1363/D3)

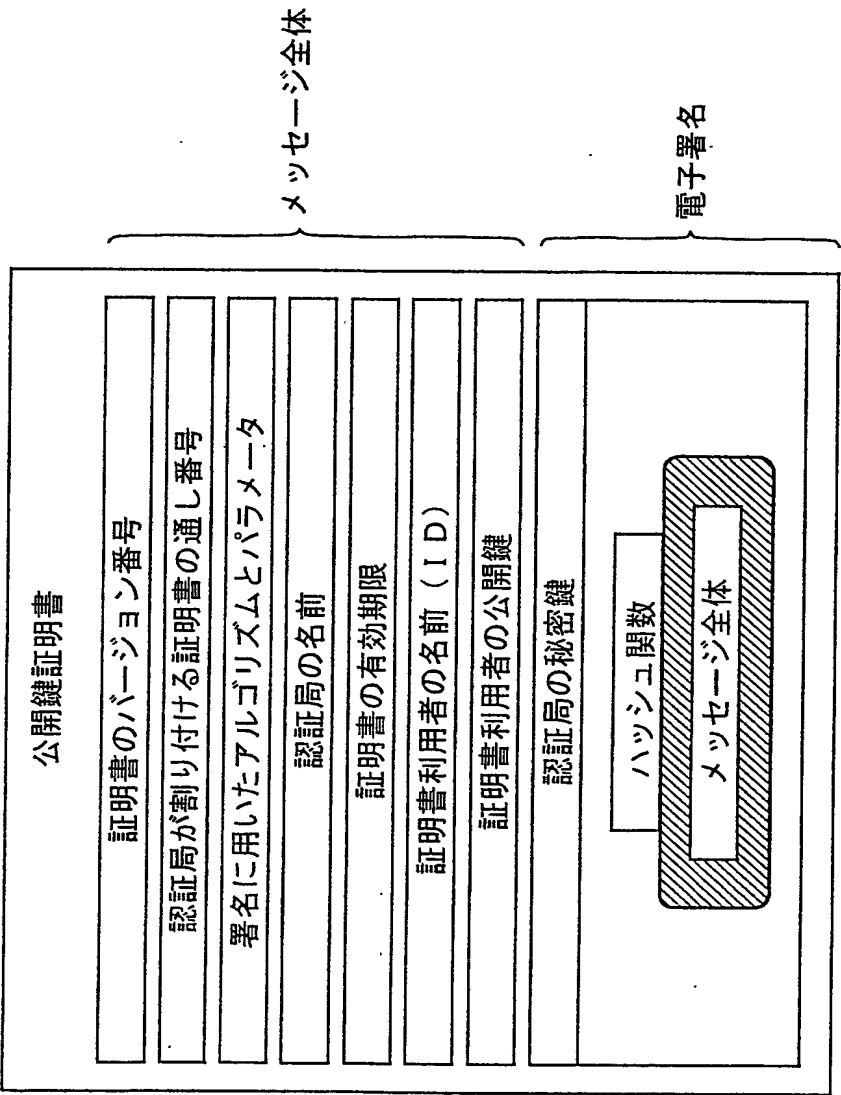
THIS PAGE BLANK (USPTO)



ISO/IEC 9798-2 対称鍵暗号鍵技術を用いた相互認証および鍵共有方式

図 13

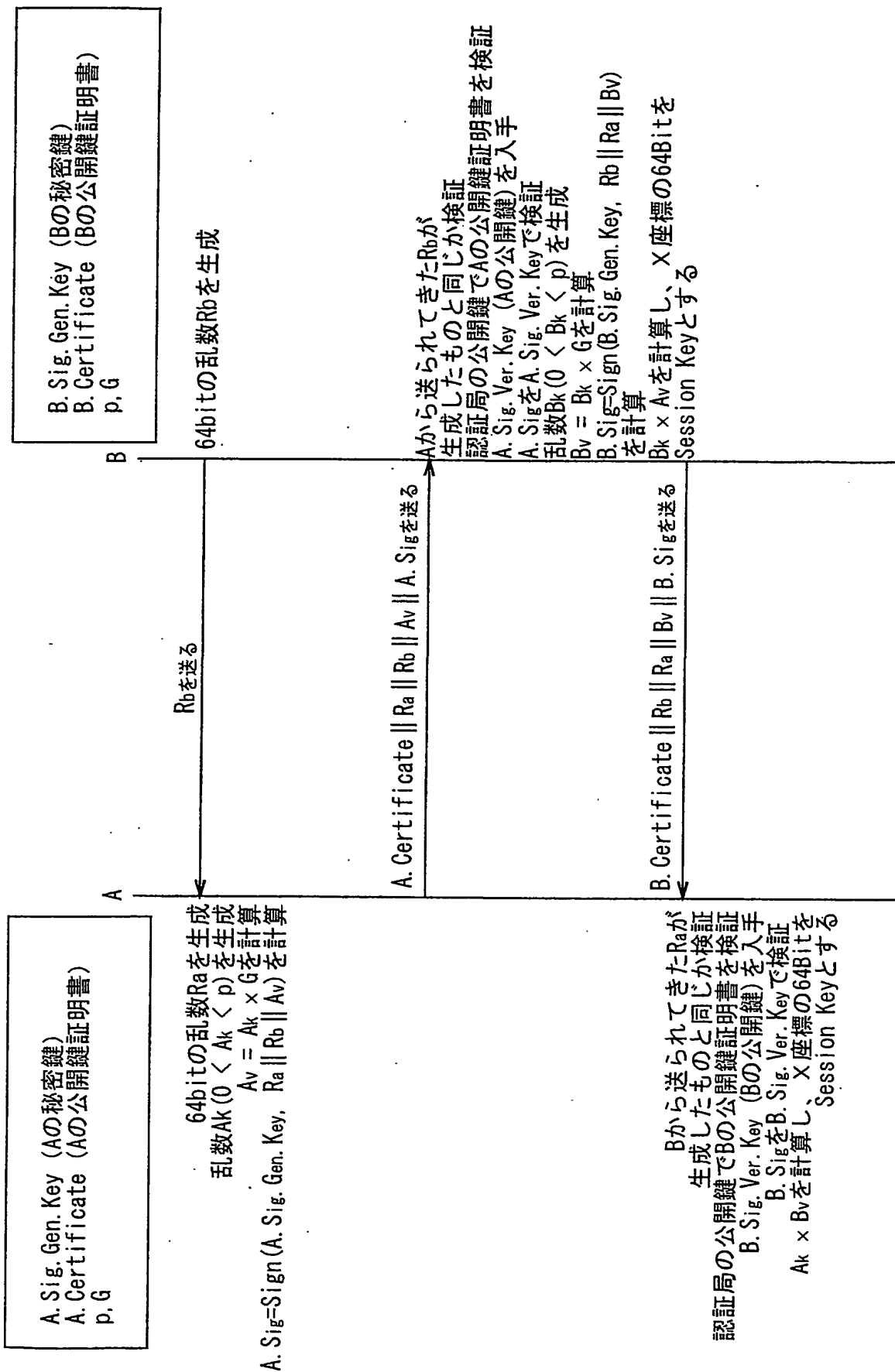
THIS PAGE BLANK (USPTO)



公開鍵証明書

図 14

THIS PAGE BLANK (USPTO)



ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

THIS PAGE BLANK (USPTO)

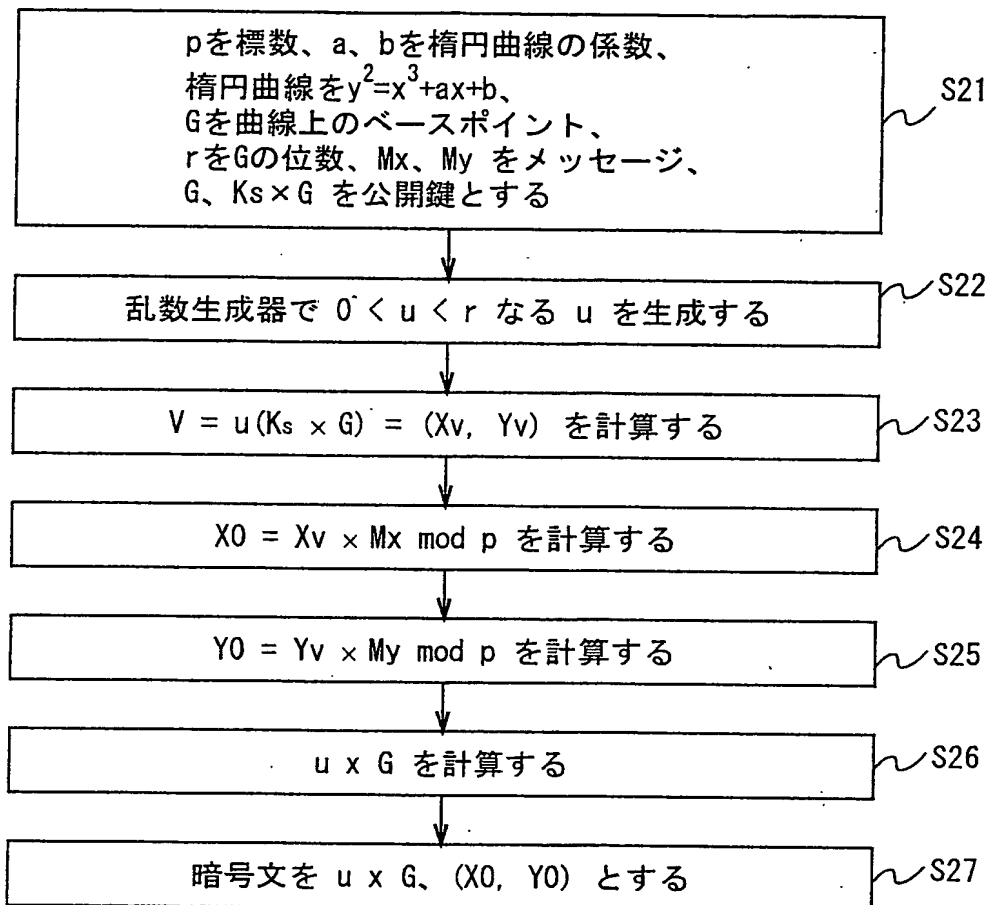
暗号化楕円曲線暗号を用いた暗号化 (Menezens-Vanstone)

図 1 6

THIS PAGE BLANK (USP10)

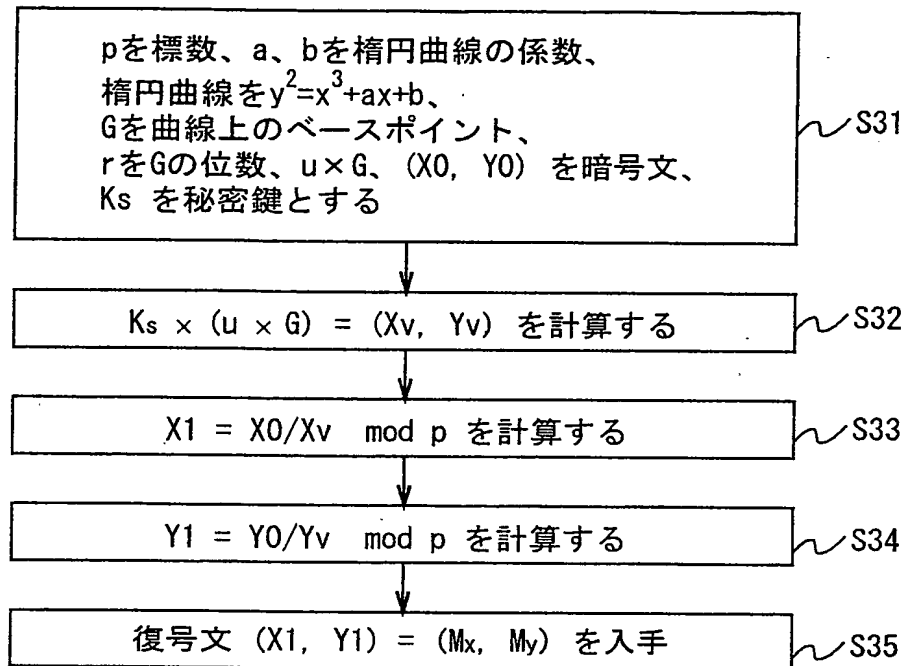
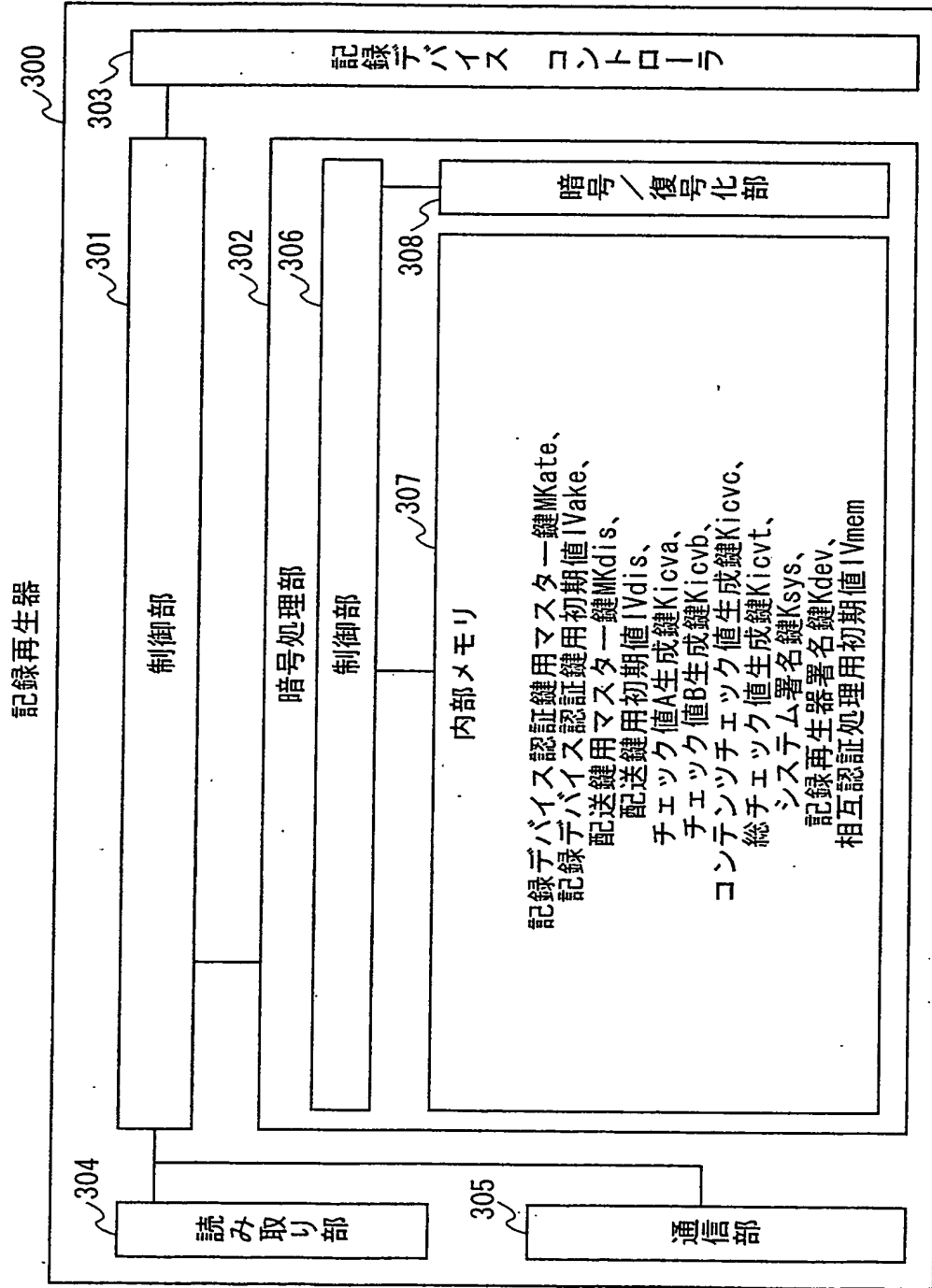
復号化楕円曲線暗号を用いた復号化 (Menezes-Vanstone)

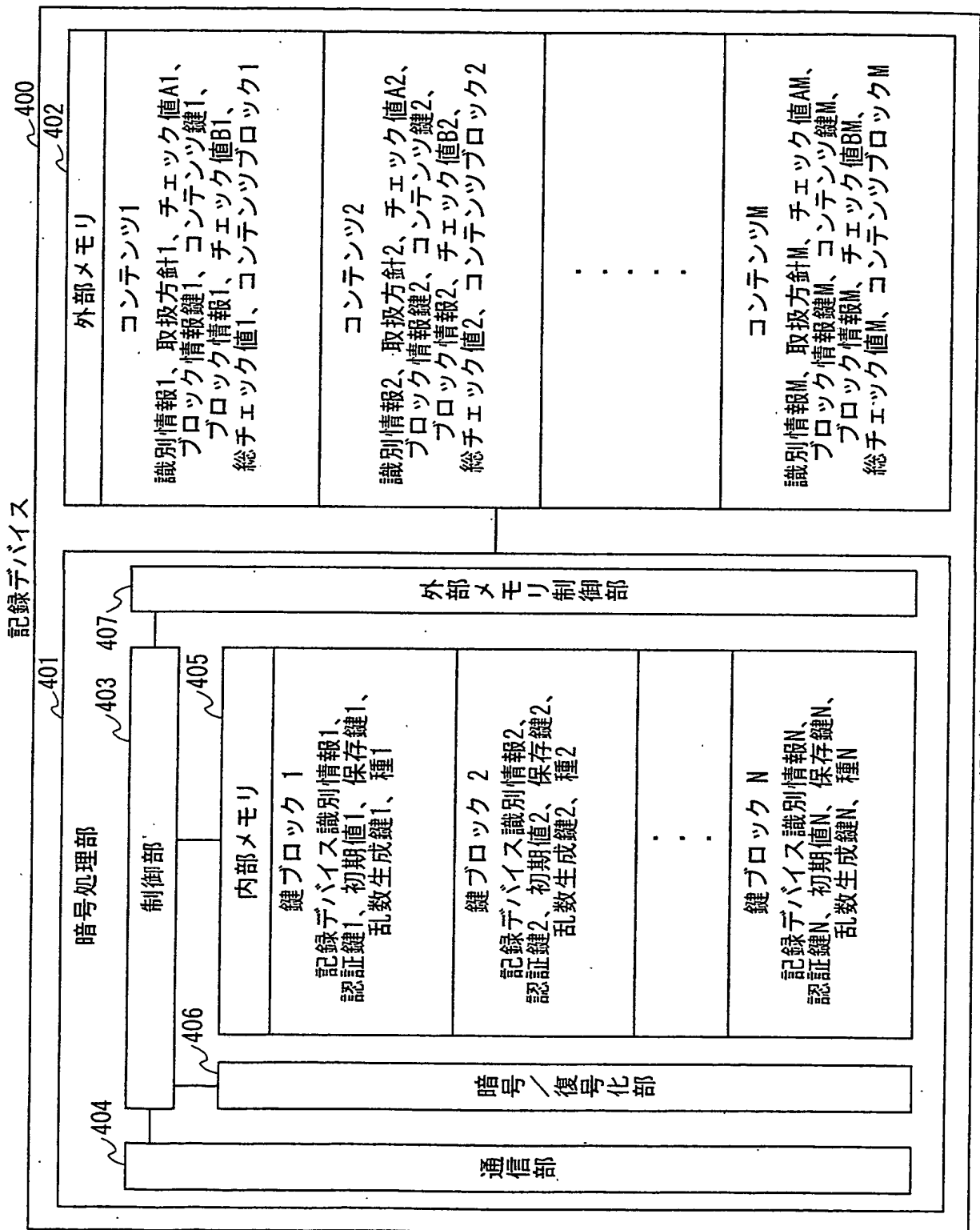
図 17

THIS PAGE BLANK (USPTO)



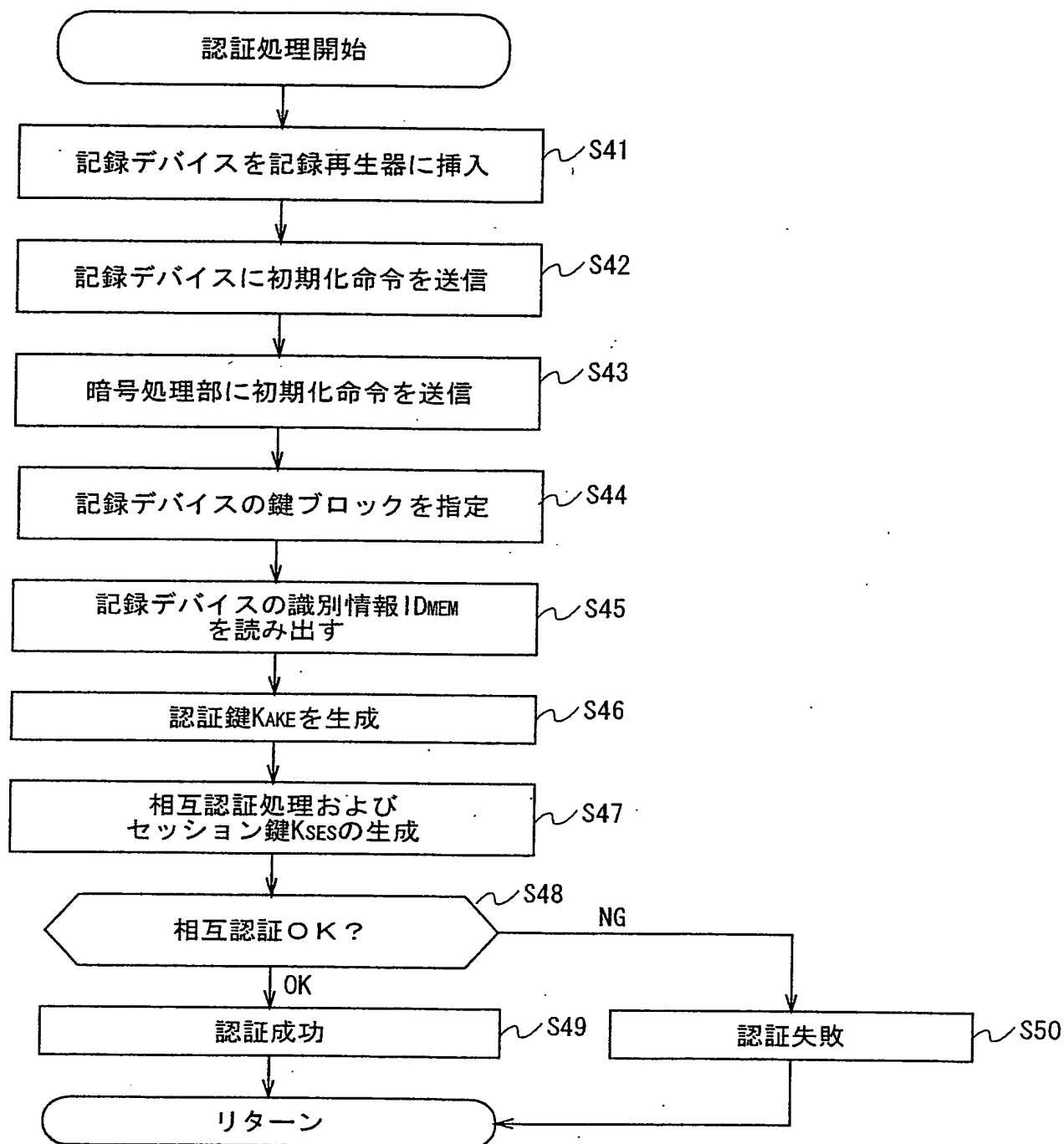
記録再生器上のデータ保持状況

THIS PAGE BLANK (USPTO)



記録デバイス上のデータ保持状況

THIS PAGE BLANK (USPTO)



記録再生器と記録デバイスとの相互認証

THIS PAGE BLANK (USPTO)

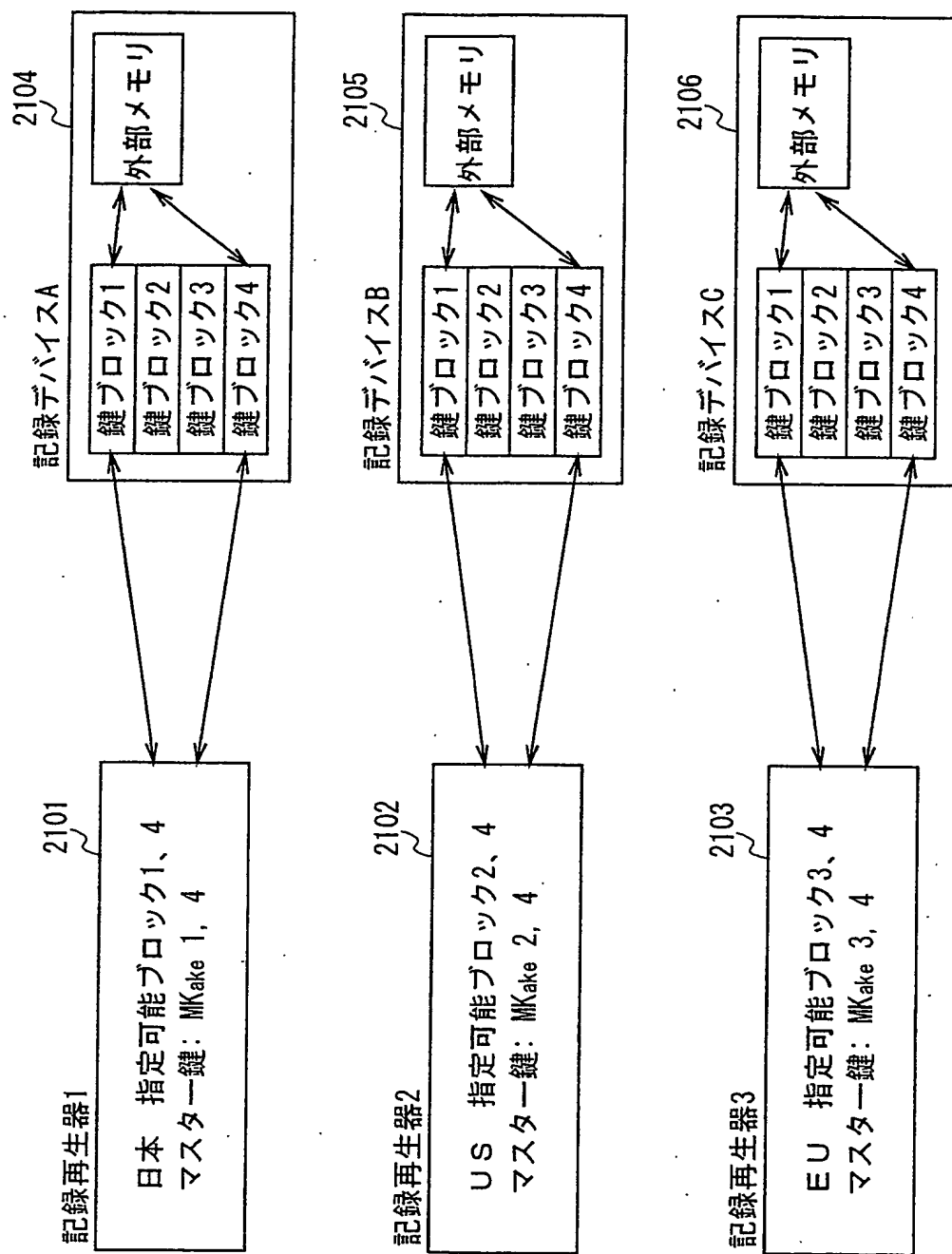


図 2 1

THIS PAGE BLANK (USPS)

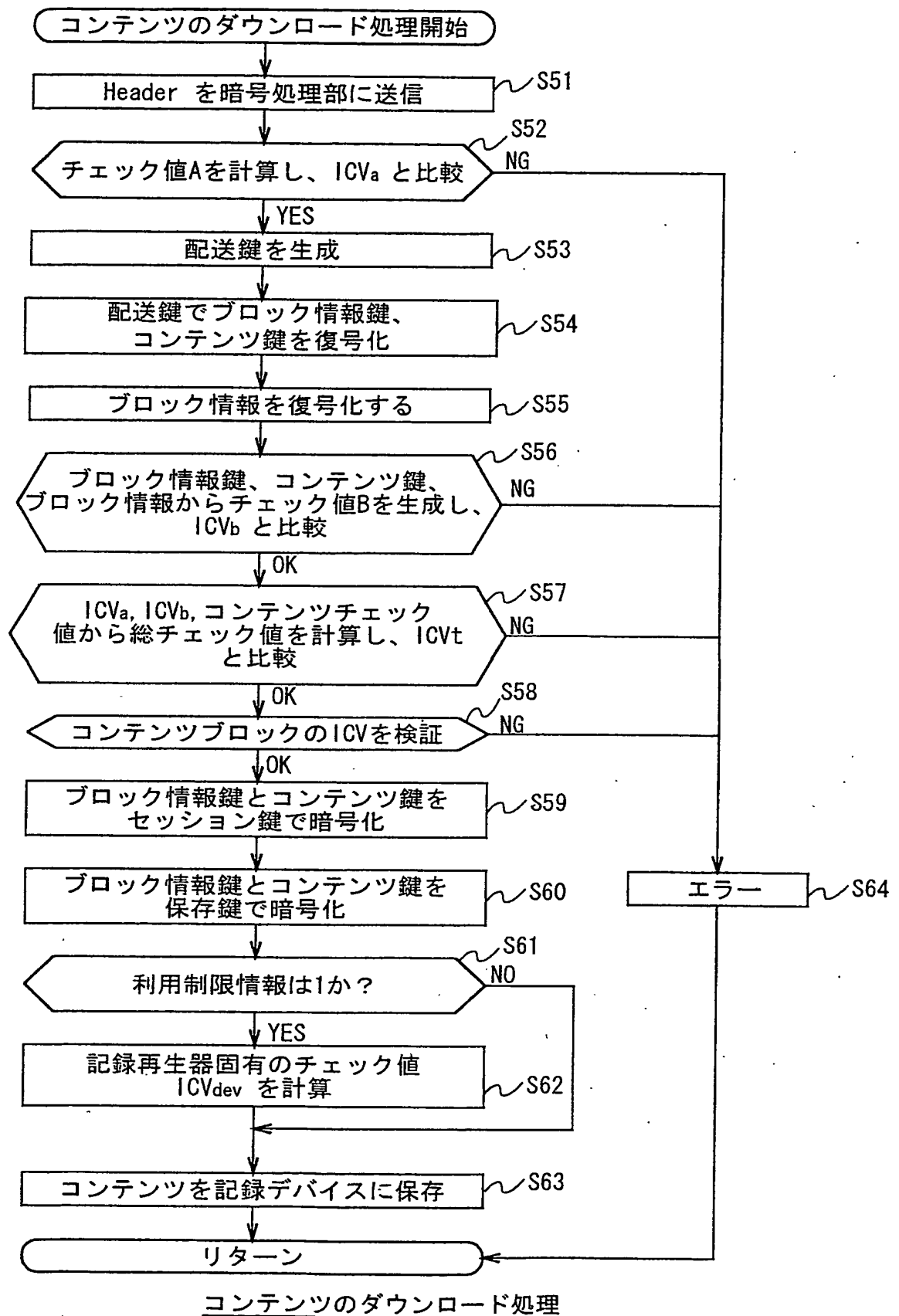


図 2 2

THIS PAGE BLANK (USPTO)

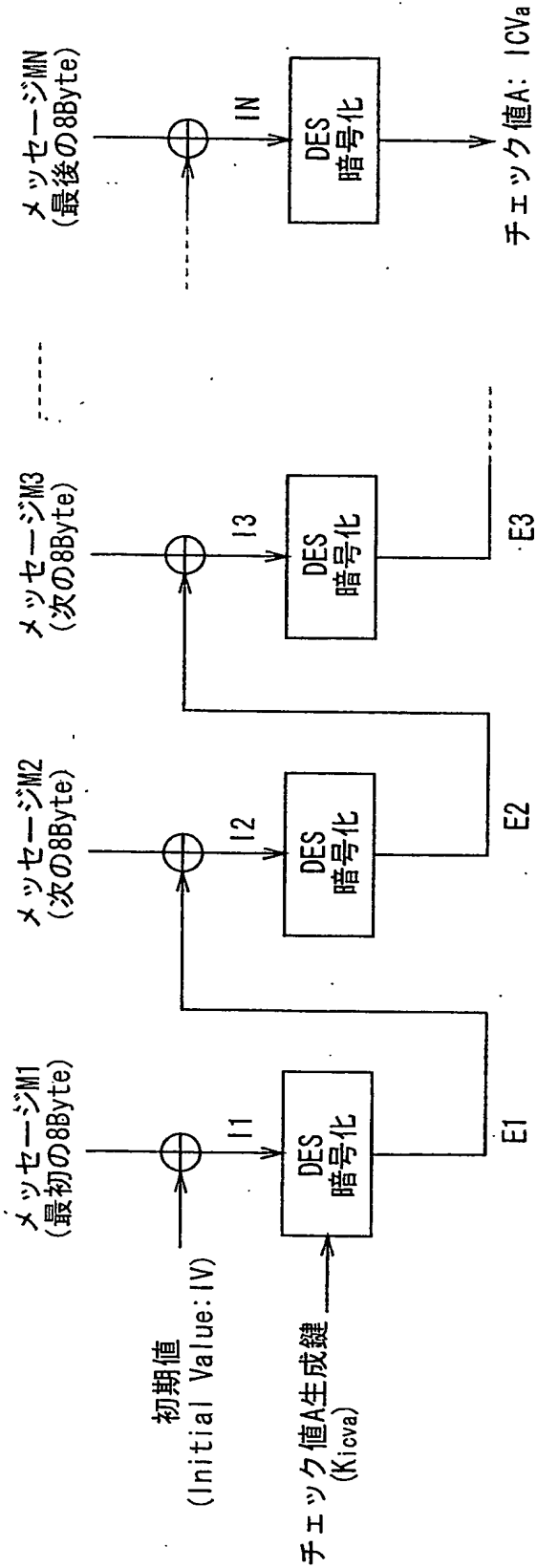
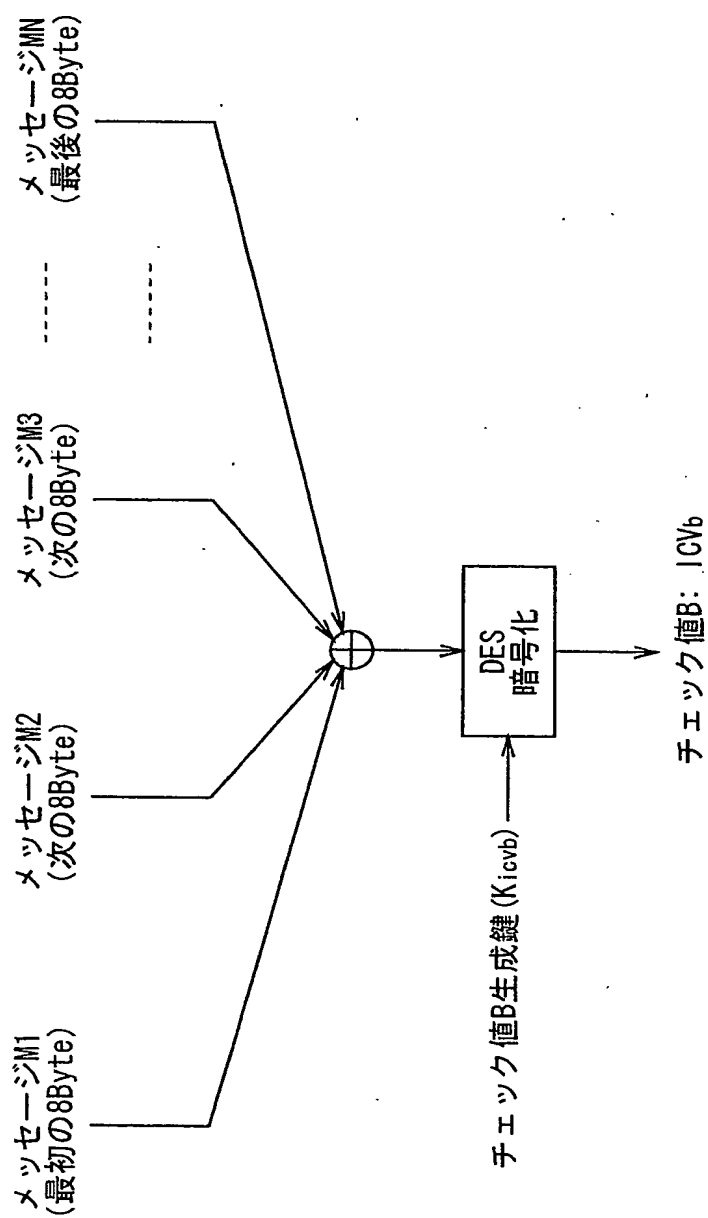


図 23

メッセージM1～MN:識別情報、取扱方針

⊕:排他的論理和処理 (8バイト単位)

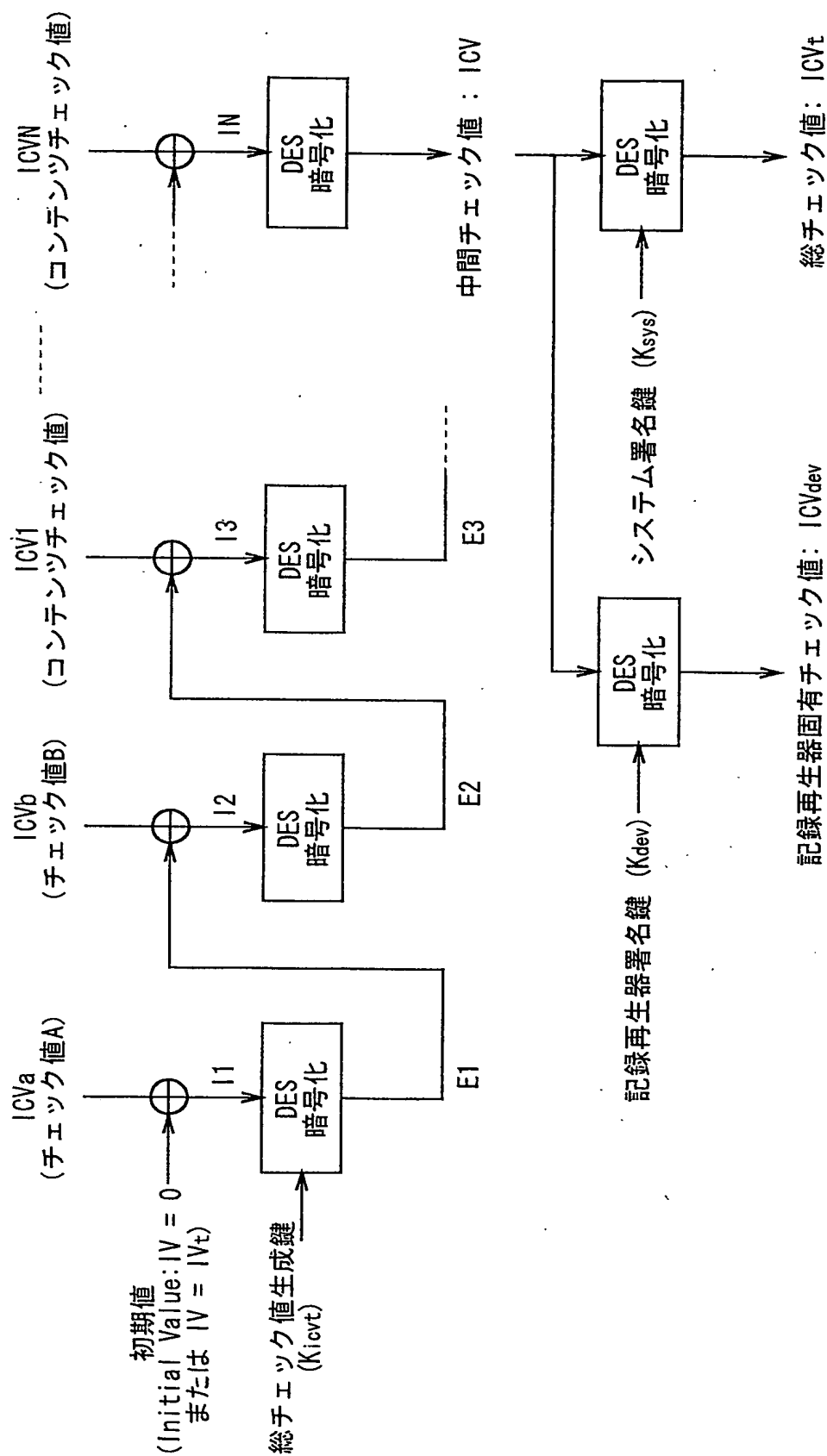
THIS PAGE BLANK (USPTO)



メッセージM1～MN：ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} 、ブロック情報
⊕:排他的論理和処理 (8バイト単位)

図 2 4

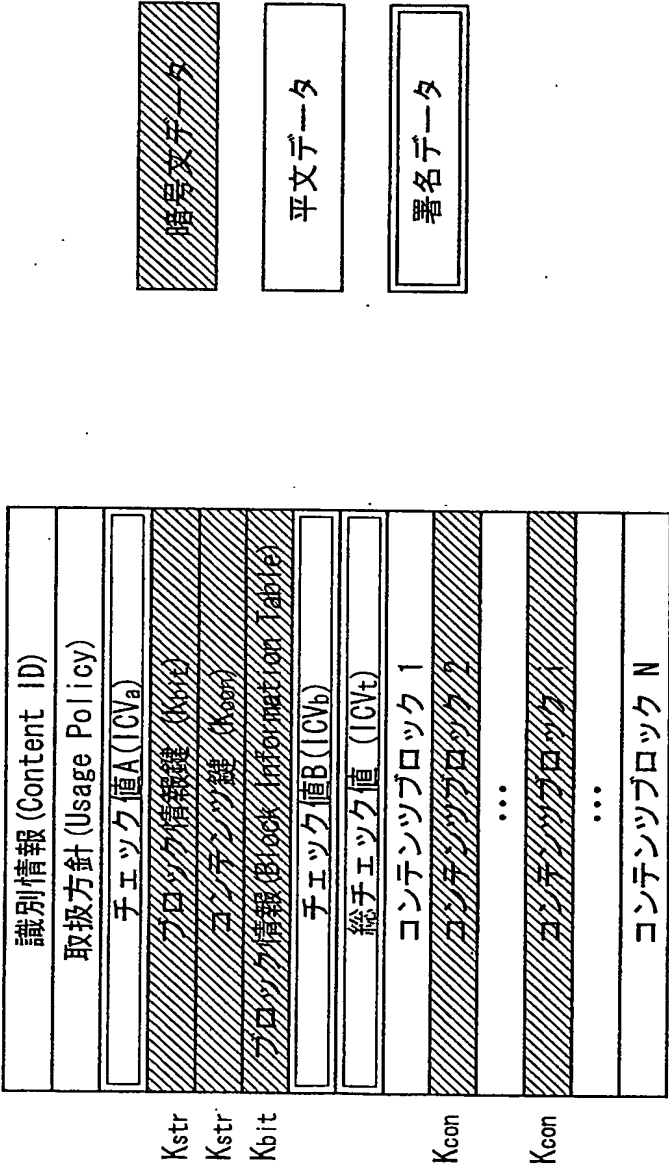
THIS PAGE BLANK (USPTO)



⊕: 排他的論理和処理 (8バイト単位)

図 25

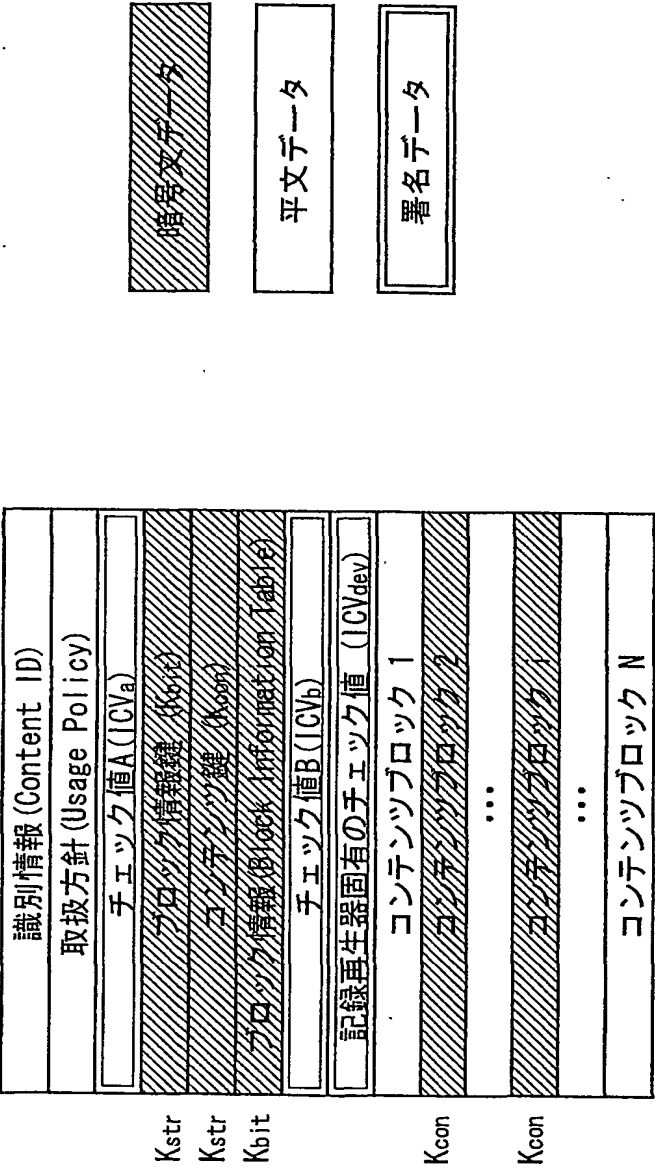
THIS PAGE BLANK (USPTO)



記録デバイスに保存されたコンテンツ
(記録制限情報 = 0)

図 26

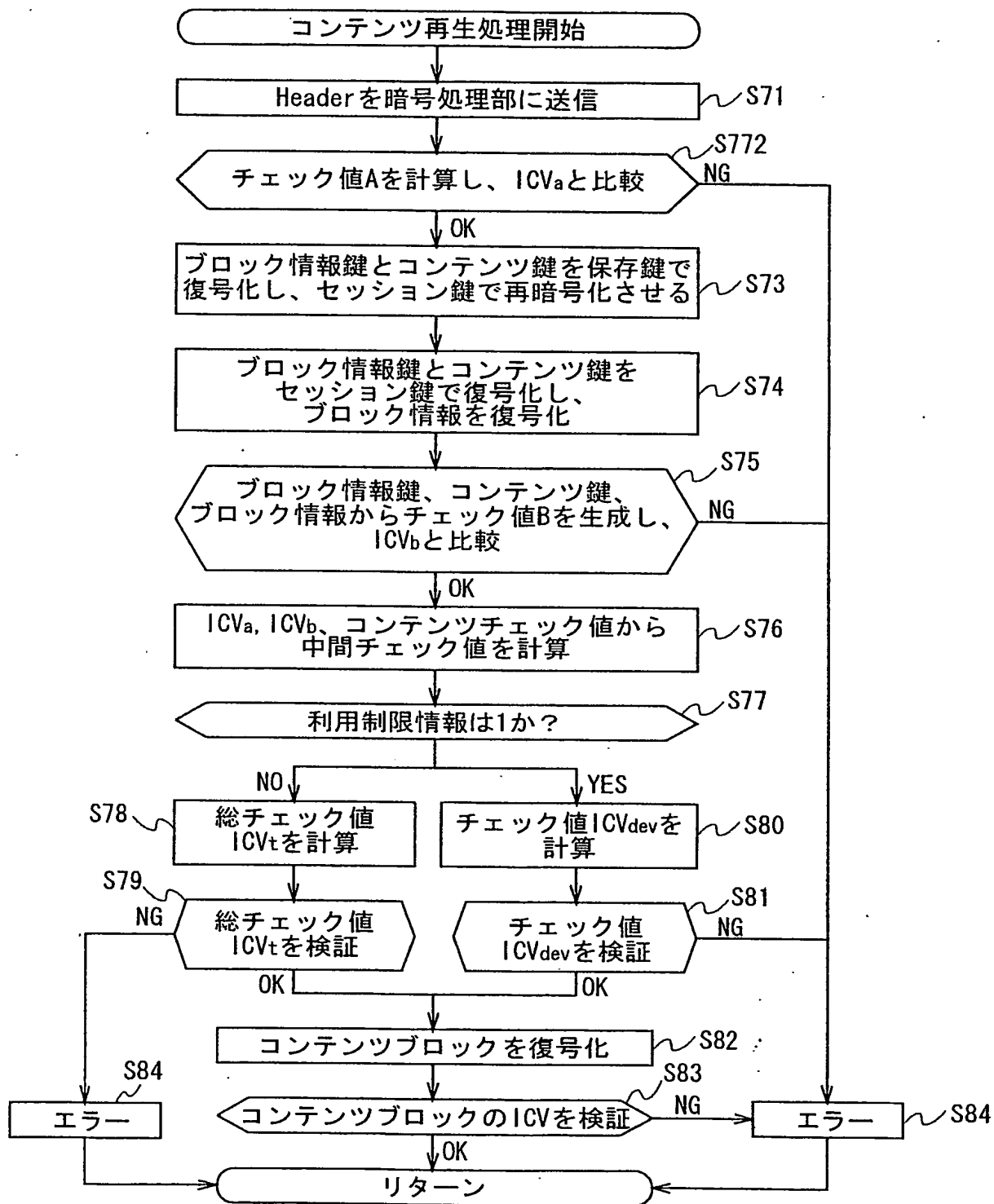
THIS PAGE BLANK (USPTO)



記録デバイスに保存されたコンテンツ
(利用制限情報 = 1)

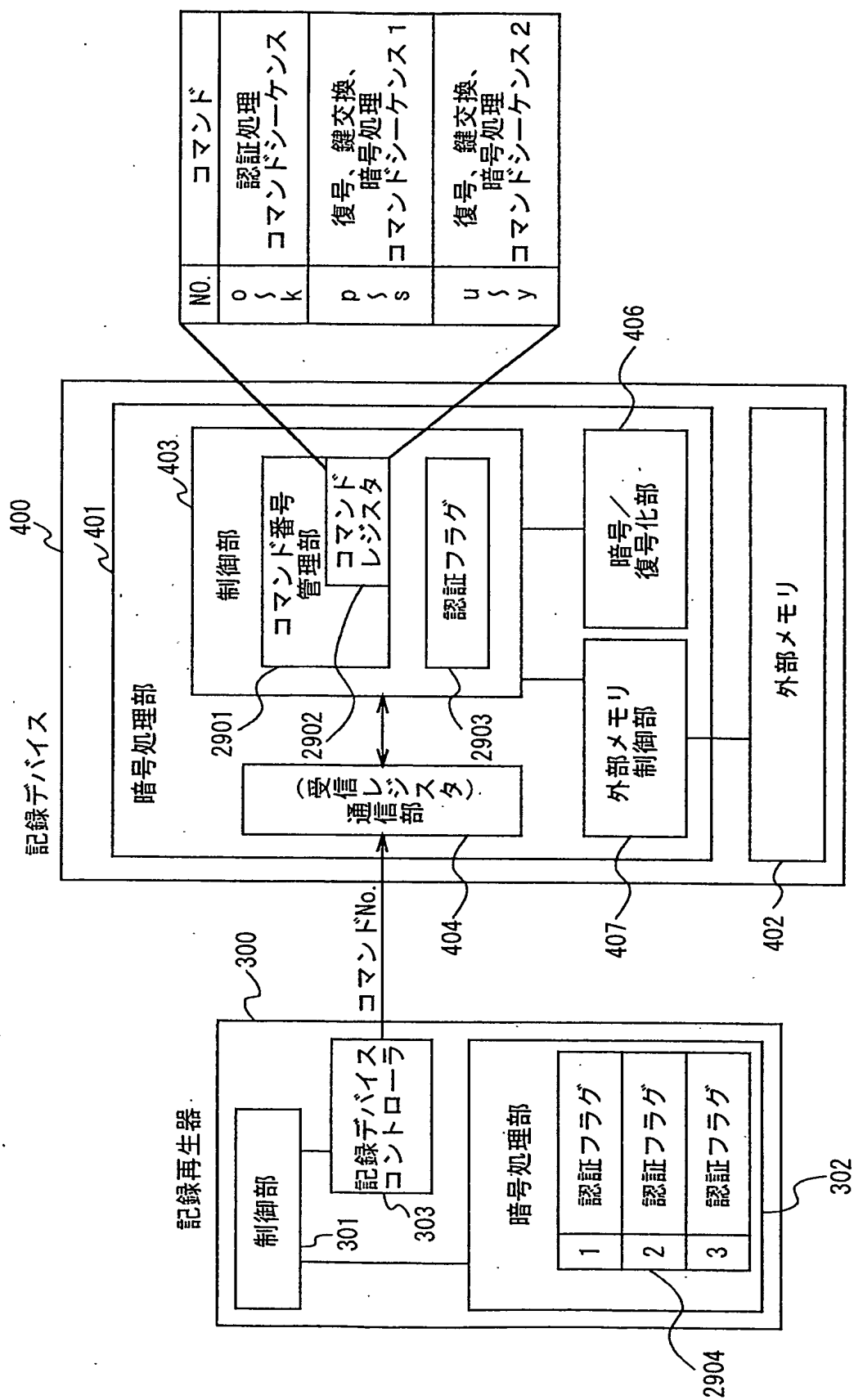
図 27

THIS PAGE BLANK (USPTO)



コンテンツの再生処理

THIS PAGE BLANK (uspto)



928

THIS PAGE BLANK (USPTO)

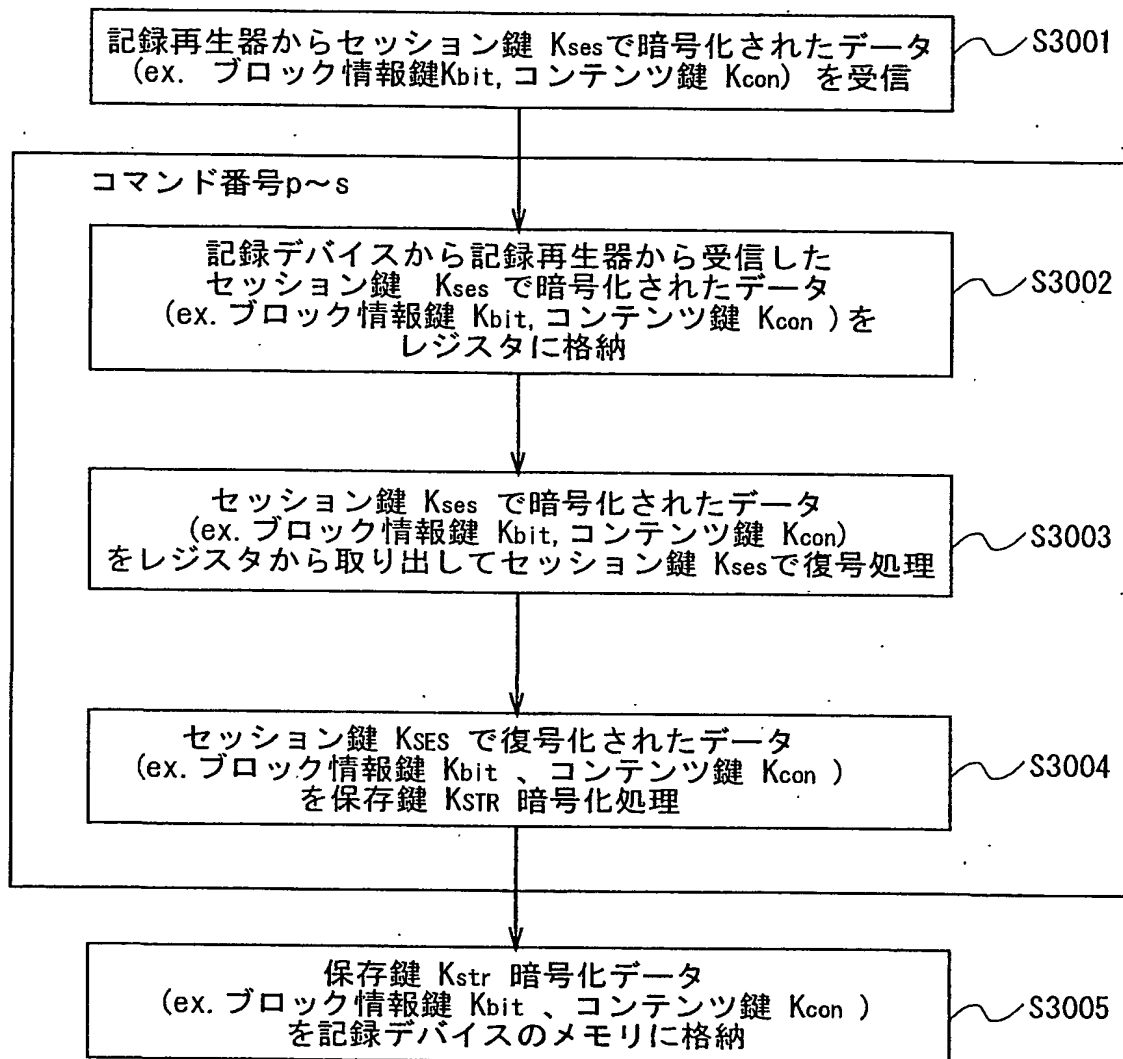


図 3 0

THIS PAGE BLANK (USPTO)

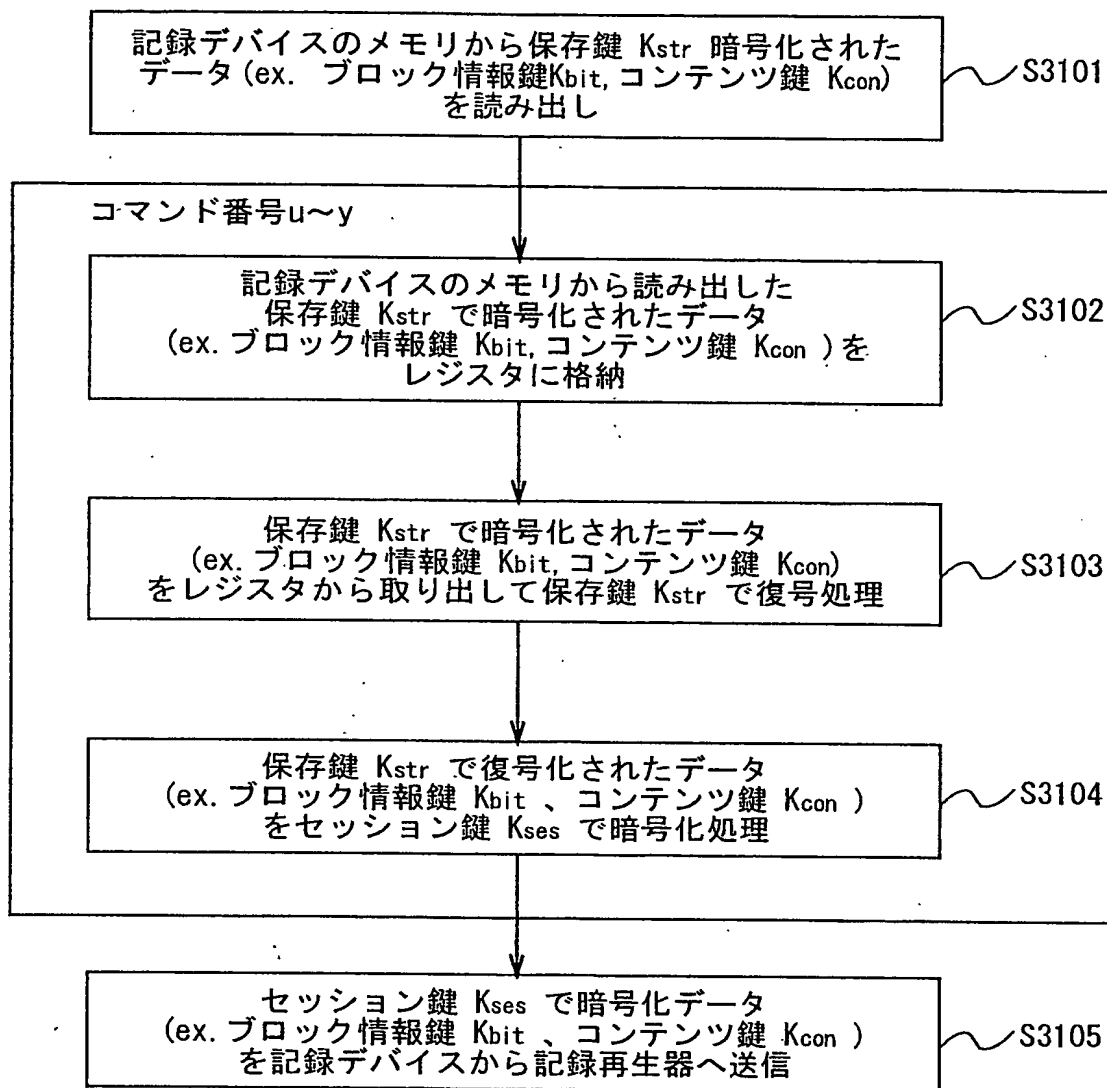


図 3 1

THIS PAGE BLANK (user)

フォーマット・タイプ0

	識別情報 (CONTENT ID)
	取扱方針 (USAGE POLICY)
	チェック値 A (ICV _a)
Kdis	ブロック情報鍵 (K _{bit})
Kdis	コンテンツ鍵 (K _{con})
Kbit	ブロック情報 (BLOCK INFORMATION TABLE)
	チェック値 B (ICV _b)
	総チェック値 (ICV _t)
	コンテンツブロック1
Kcon	コンテンツブロック2
	...
Kcon	コンテンツブロックN
	...
	コンテンツブロックN

メディア上及び通信路上のデータフォーマット



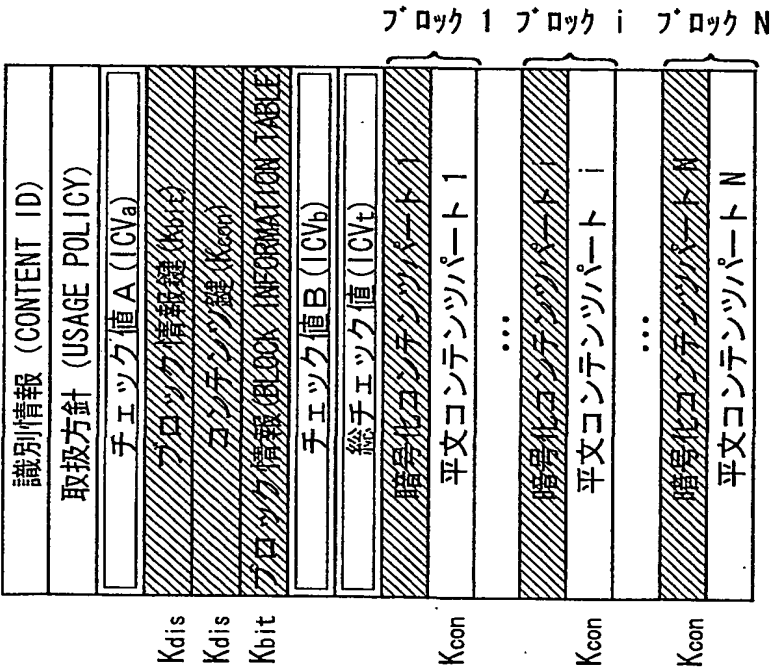
図 3 2

	識別情報 (CONTENT ID)
	取扱方針 (USAGE POLICY)
	チェック値 A (ICV _a)
Kstr	ブロック情報鍵 (K _{bit})
Kstr	コンテンツ鍵 (K _{con})
Kbit	ブロック情報 (BLOCK INFORMATION TABLE)
	チェック値 B (ICV _b)
	総チェック値 (ICV _t) or 固有チェック値 (ICV _{dev})
	コンテンツブロック1
Kcon	コンテンツブロック2
	...
Kcon	コンテンツブロックN
	...
	コンテンツブロックN

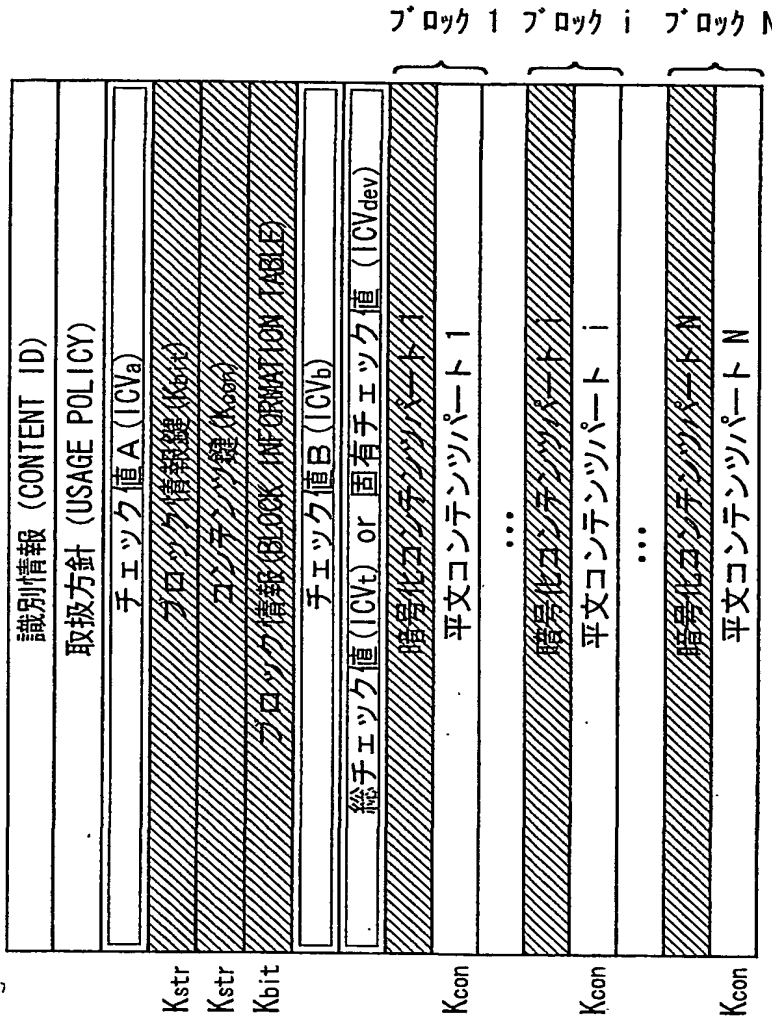
記録デバイスに保存されたコンテンツ

THIS PAGE BLANK (USPTO)

フォーマット・タイプ 1



メディア上及び通信路上のデータフォーマット



記録デバイスに保存されたコンテンツ

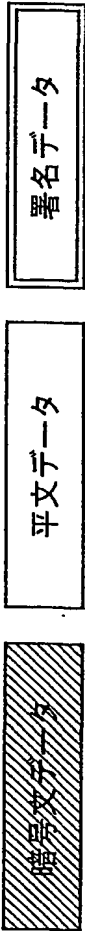
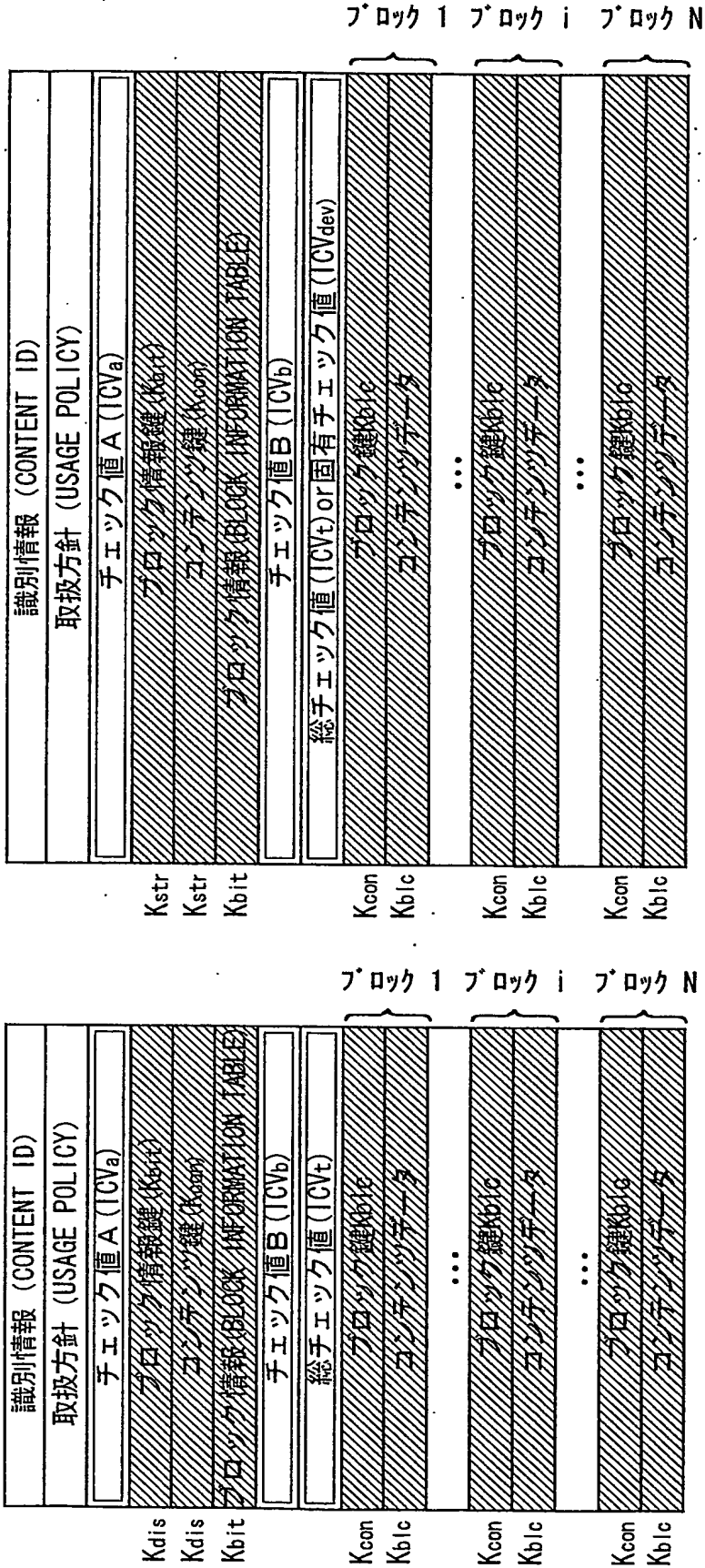


図 33

THIS PAGE BLANK (USTPTO)

フォーマット・タイプ2



記録デバイスに保存されたコンテンツ

メディア上及び通信路上のデータフォーマット

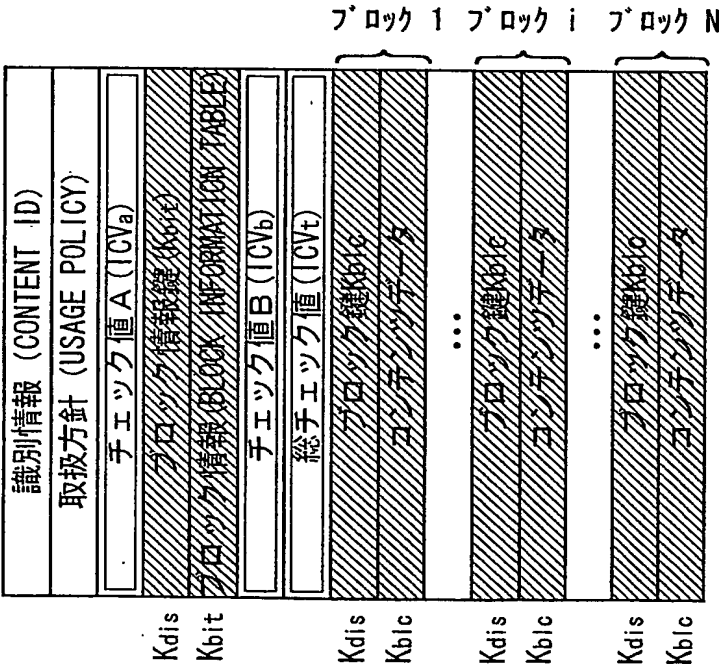
暗号文データ

署名データ

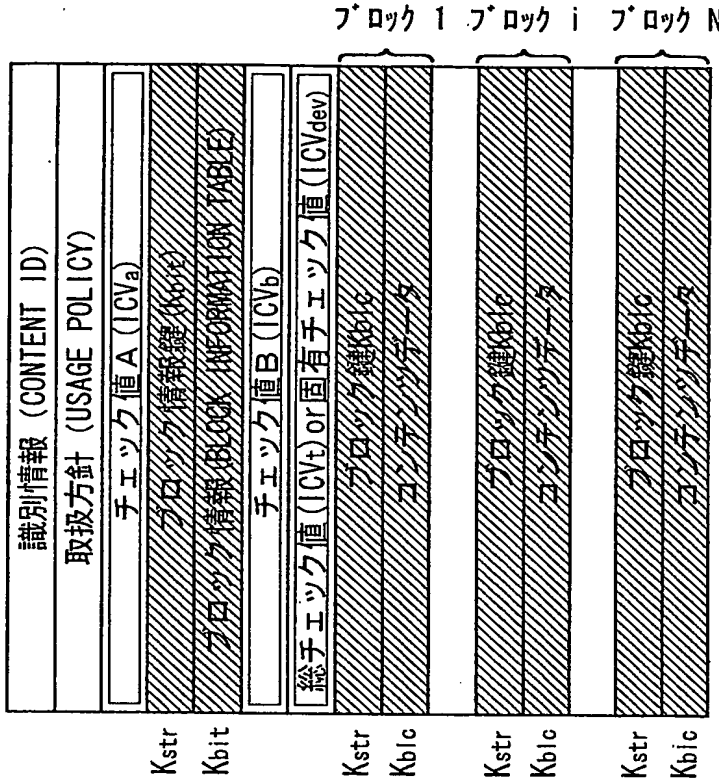
図34

THIS PAGE BLANK (USPS-10)

フォーマット・タイプ3



メディア上及び通信路上のデータフォーマット



記録デバイスに保存されたコンテンツ

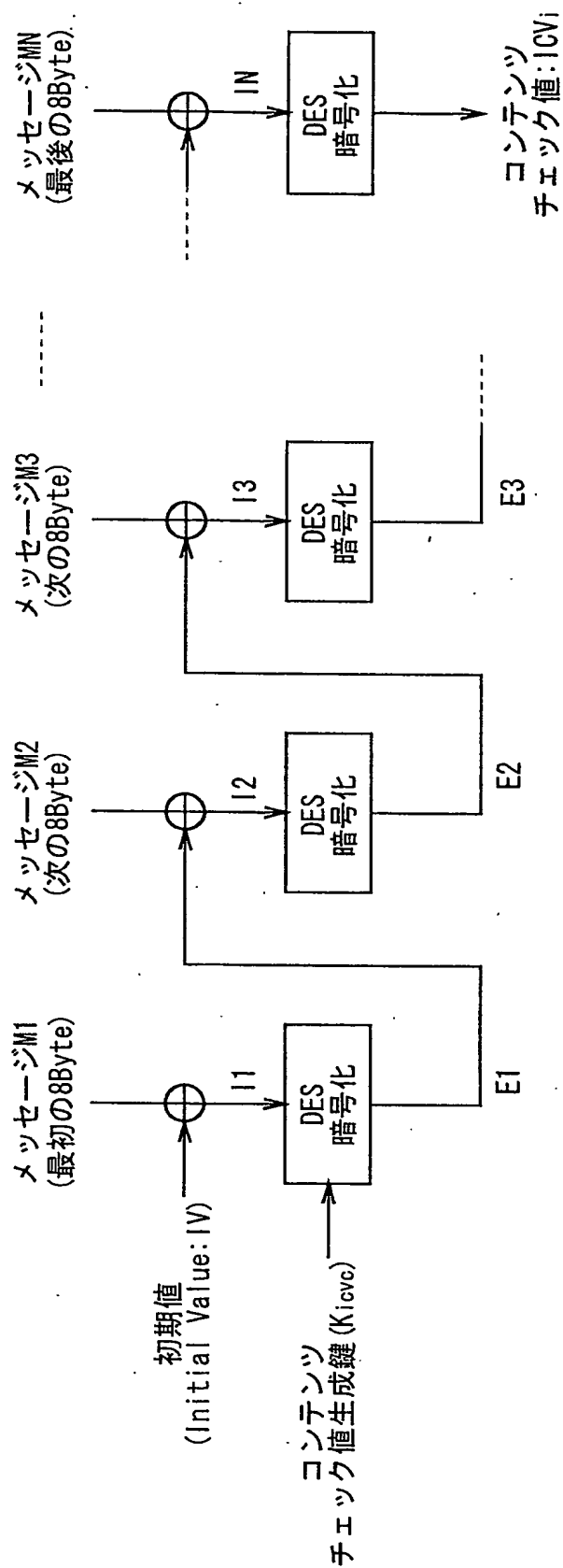
暗号文データ

平文データ

署名データ

図 35

THIS PAGE BLANK (USPS)

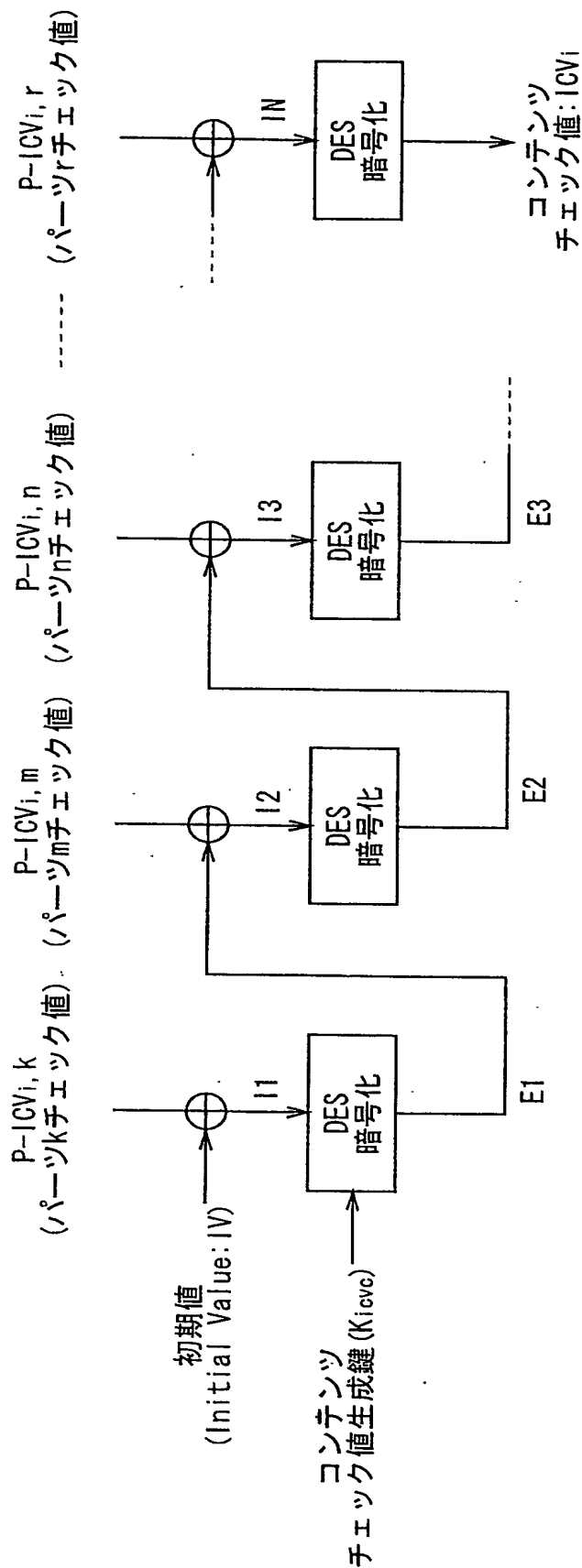


メッセージM1～MN:コンテンツのコンテンツデータ

⊕:排他的論理和処理 (8バイト単位)

図 3 6

THIS PAGE BLANK (uspto)



⊕:排他的論理和処理 (8バイト単位)

図 37

THIS PAGE BLANK (USPTO)

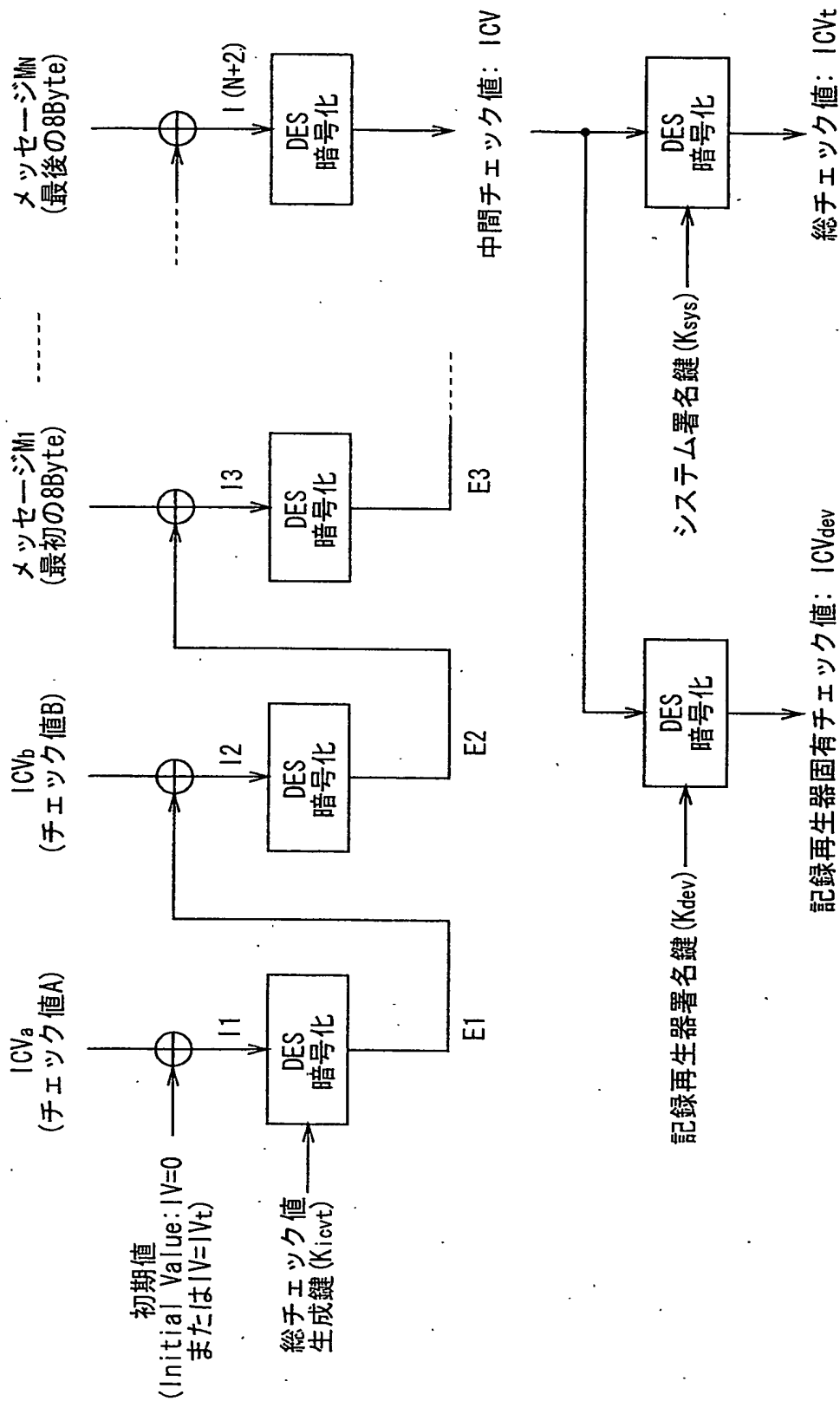


図 38

THIS PAGE BE BLANK (uspto)

フォーマットタイプ0、1ダウンロード処理

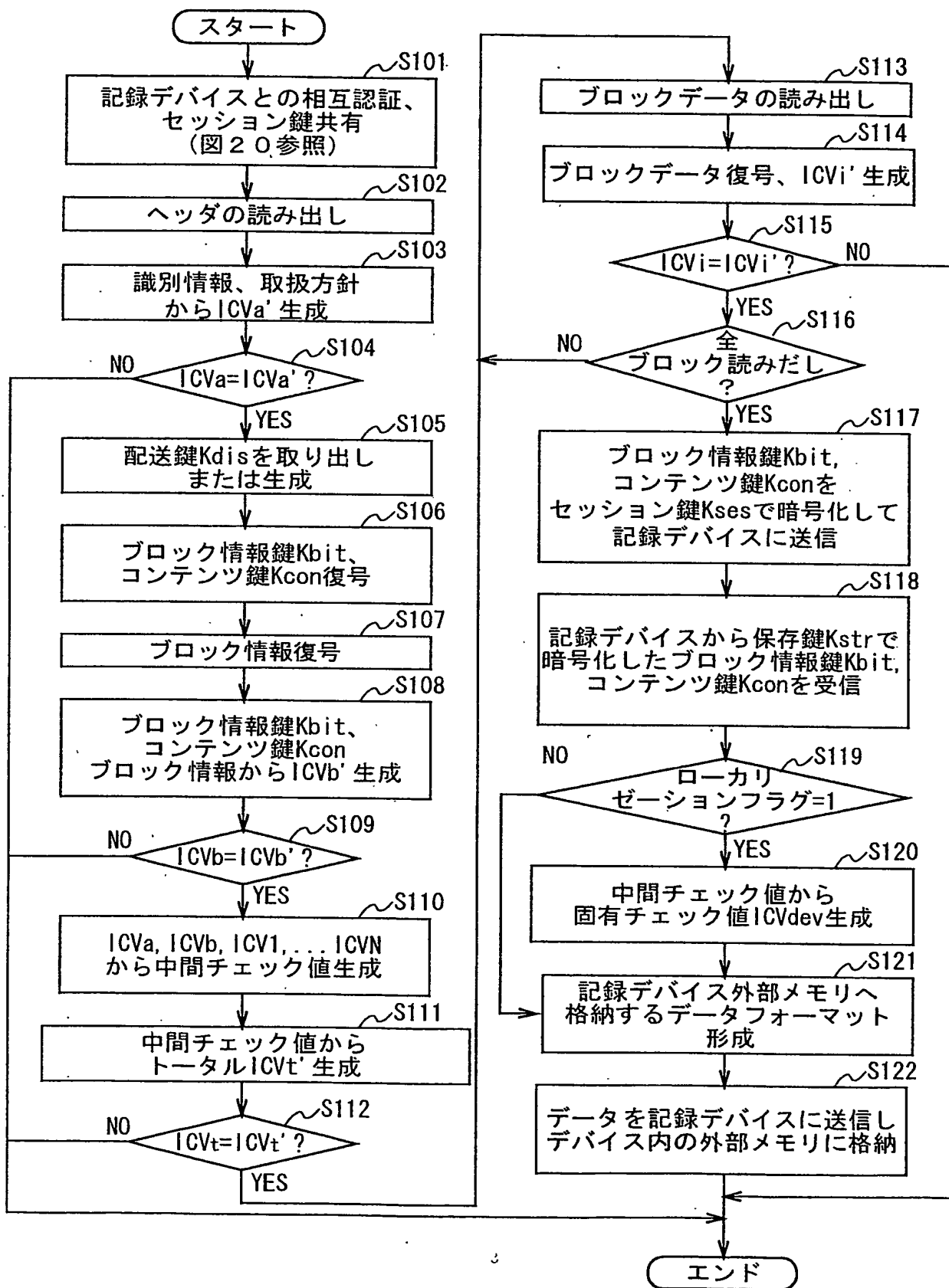


図39

THIS PAGE BLANK (USPTO)

フォーマットタイプ2ダウンロード処理

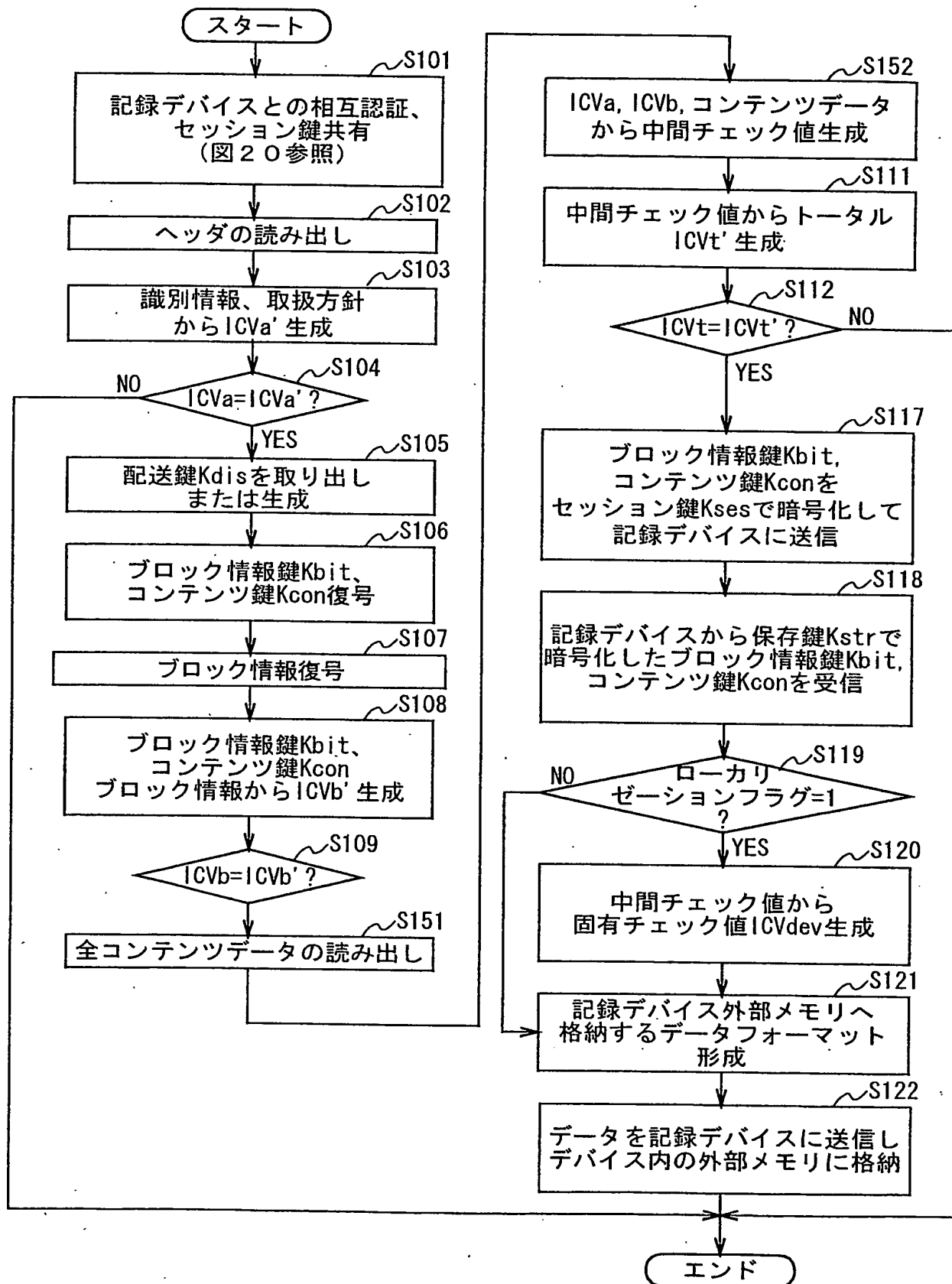


図40

THIS PAGE BLANK (USPTO)

フォーマットタイプ3ダウンロード処理

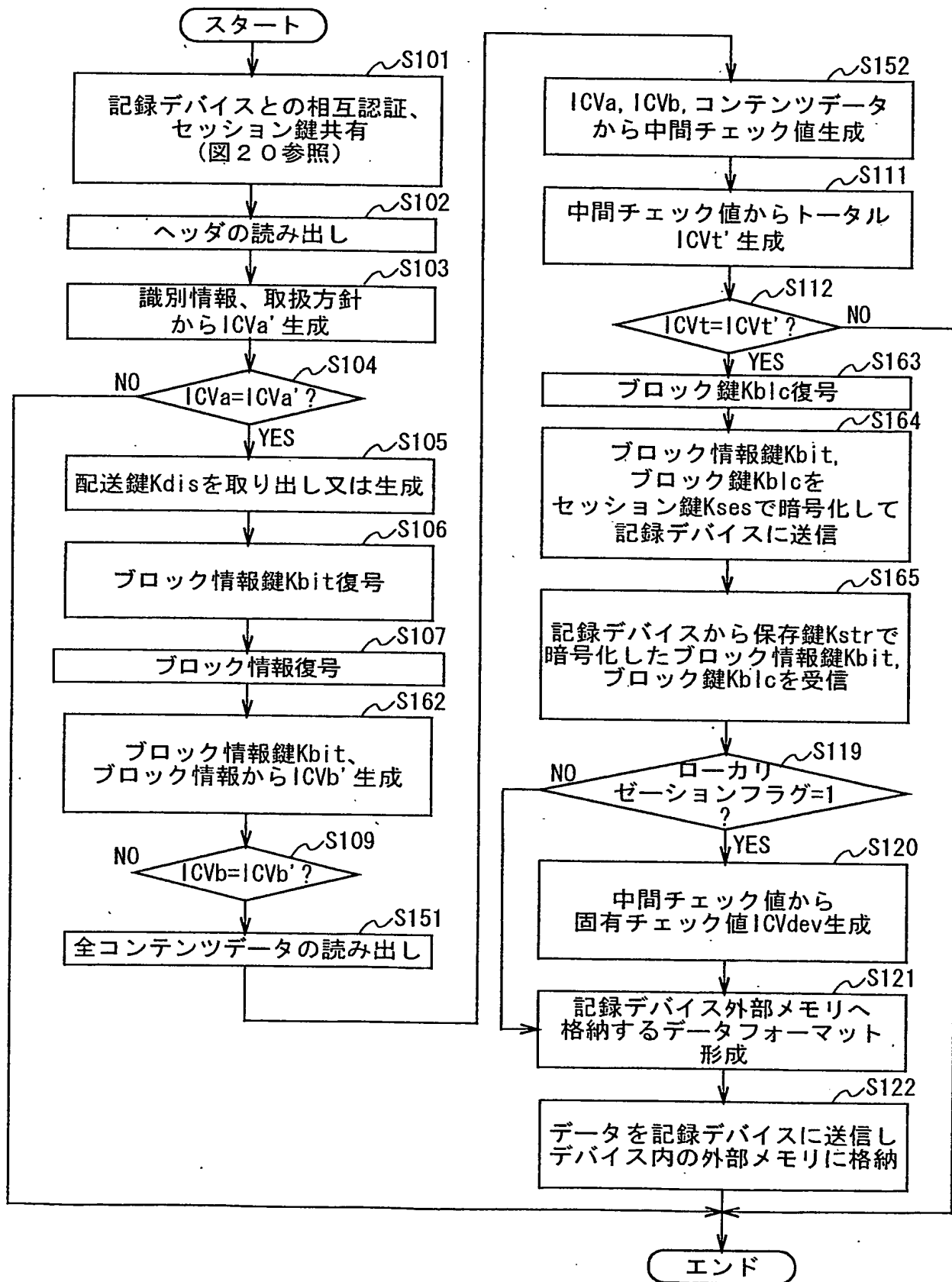


図4 1

THIS PAGE BLANK (USPTO)

フォーマットタイプ0再生処理

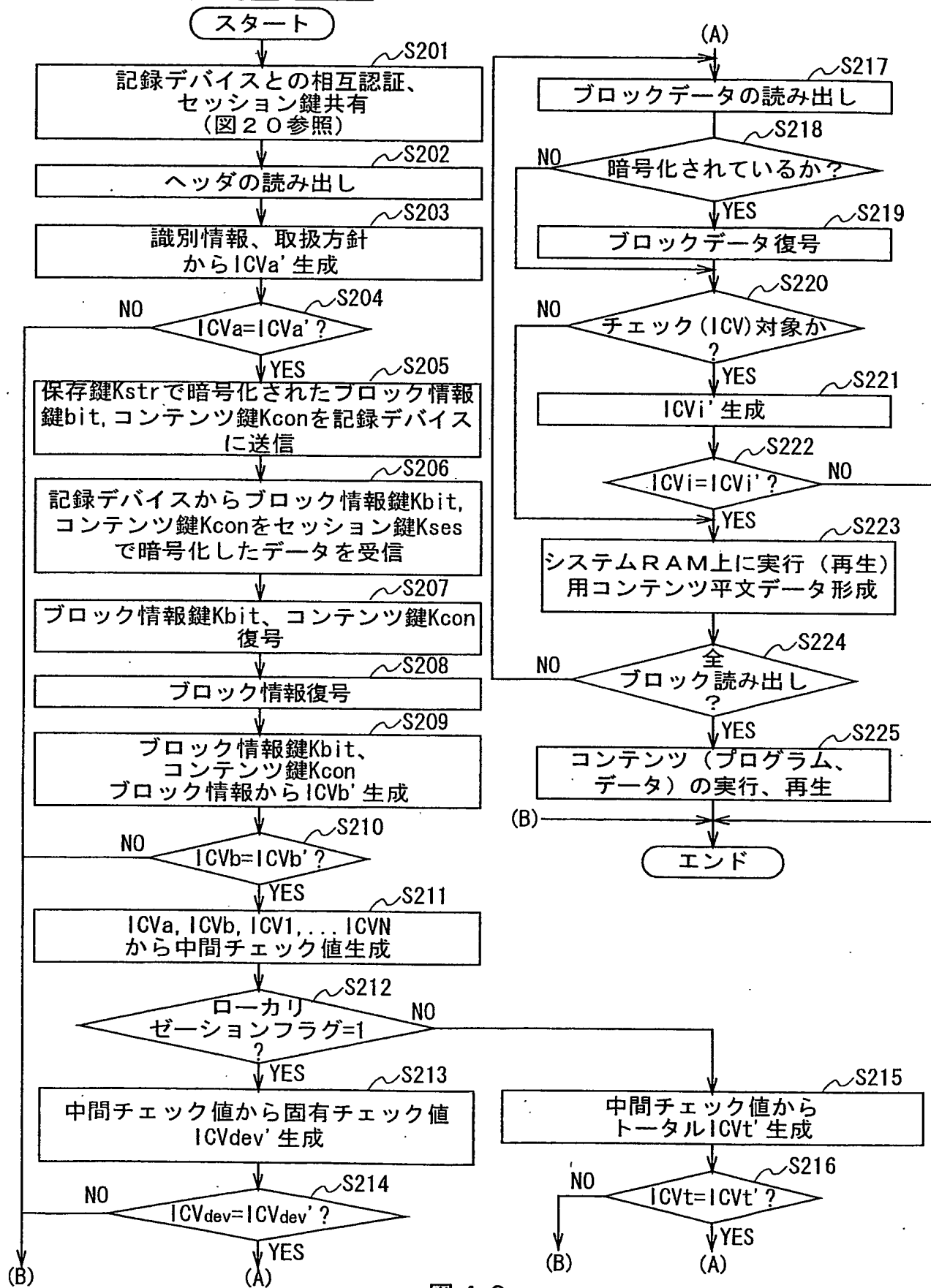


图 4 2

THIS PAGE BLANK (USPTO)

フォーマットタイプ1再生処理

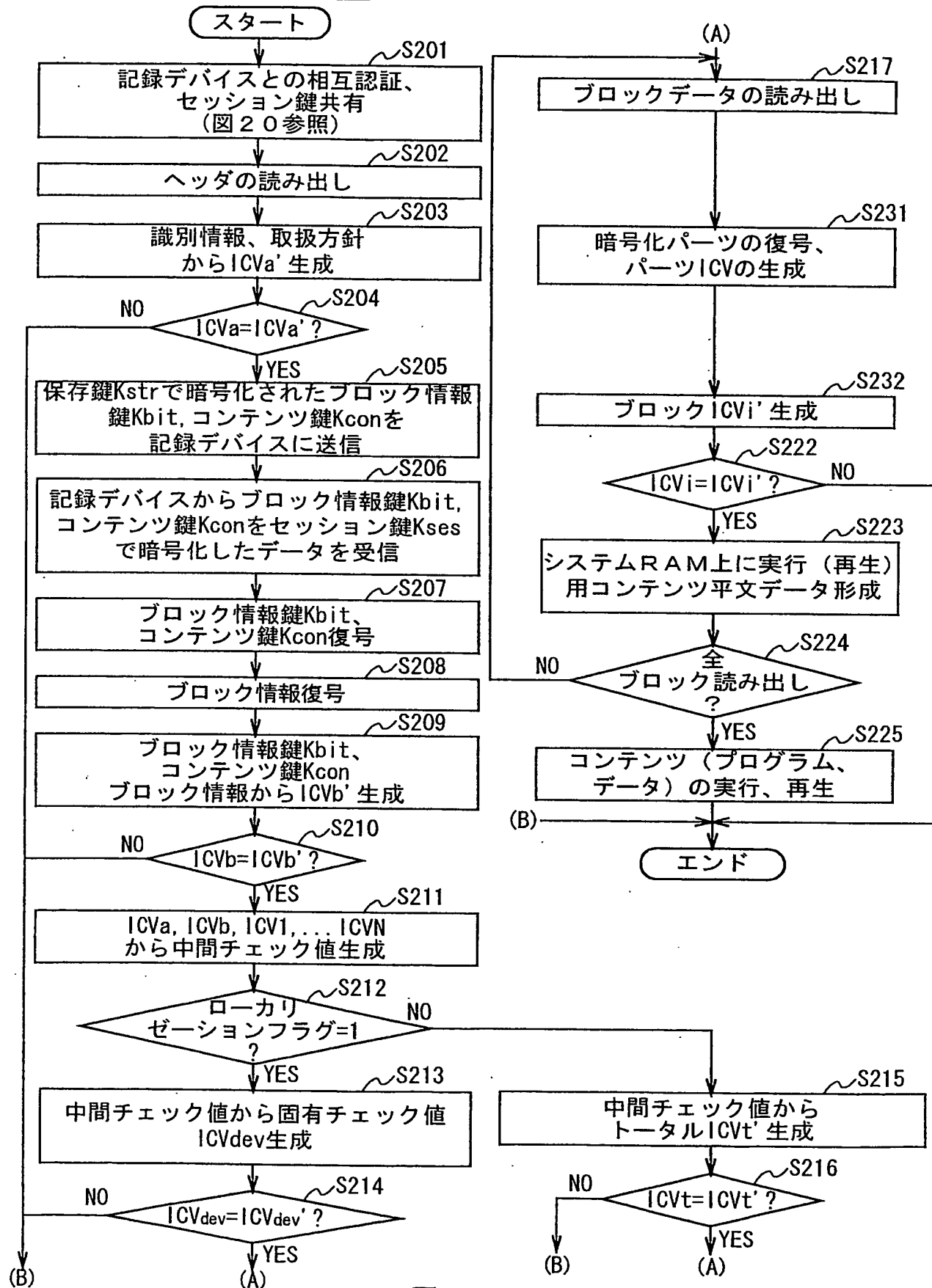


図43

THIS PAGE BEGINS BLANK (USPTO)

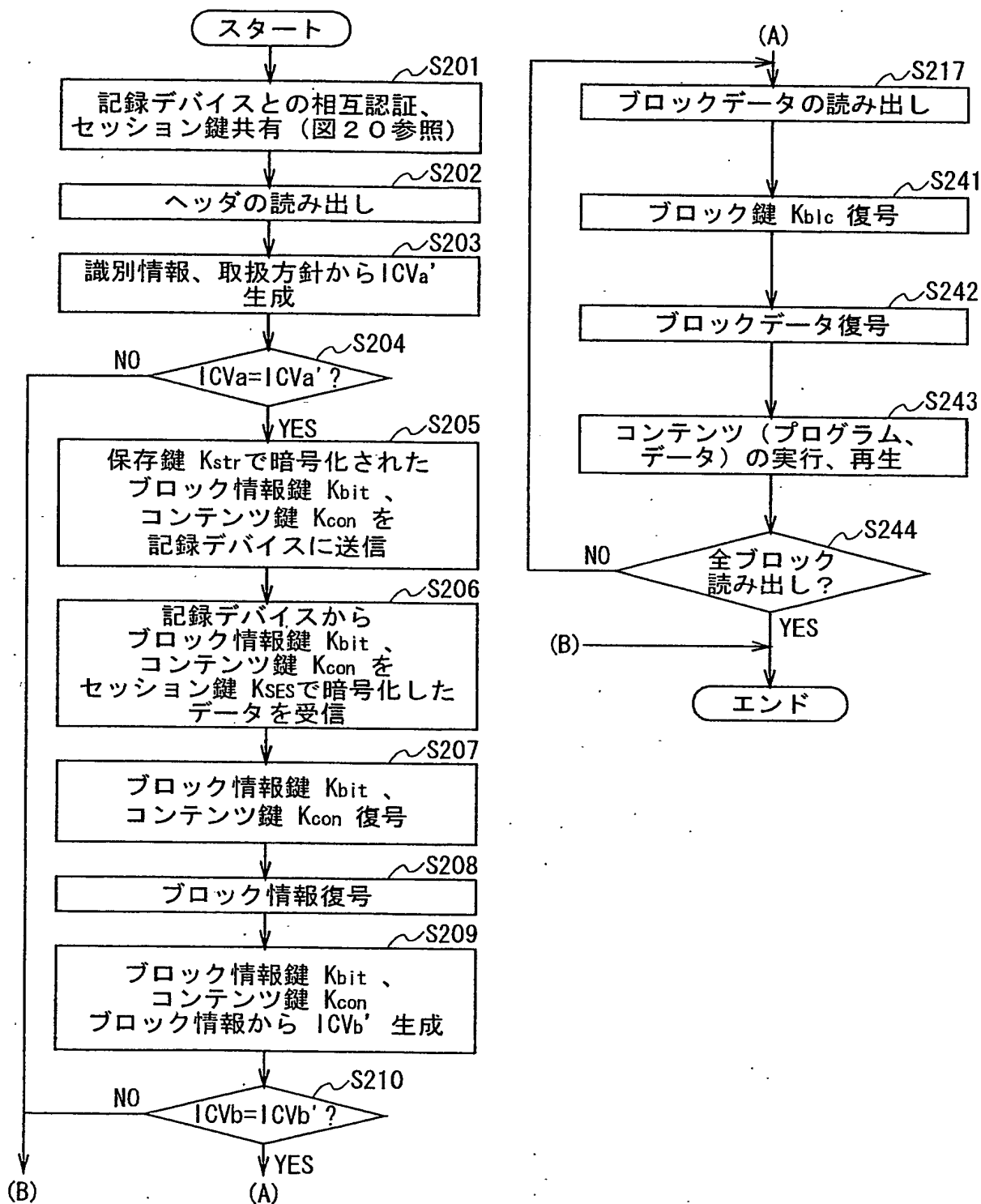


図 4 4

THIS PAGE BLANK (USPTO)

フォーマットタイプ3再生処理

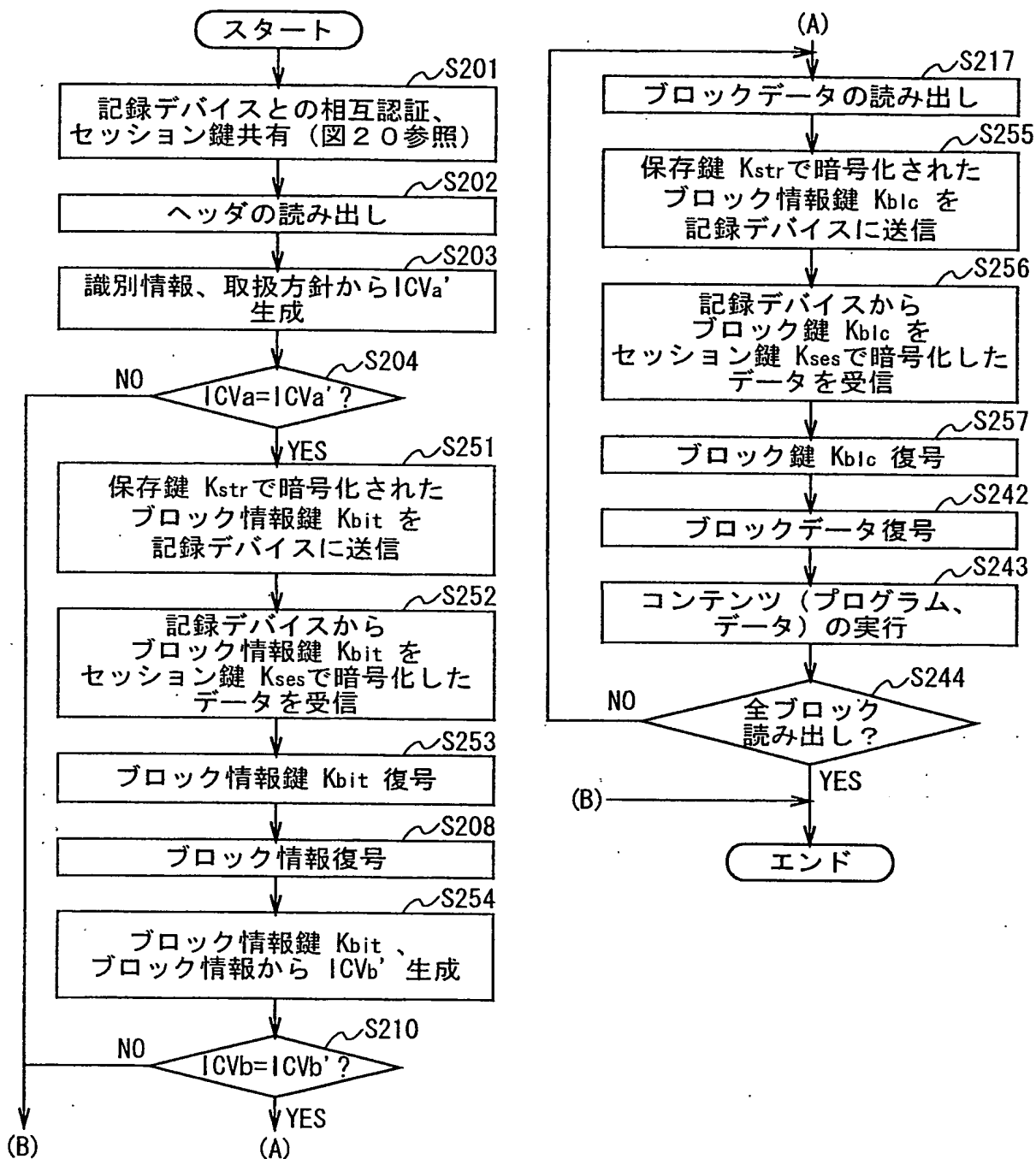


図 4 5

THIS PAGE BLANK (user)

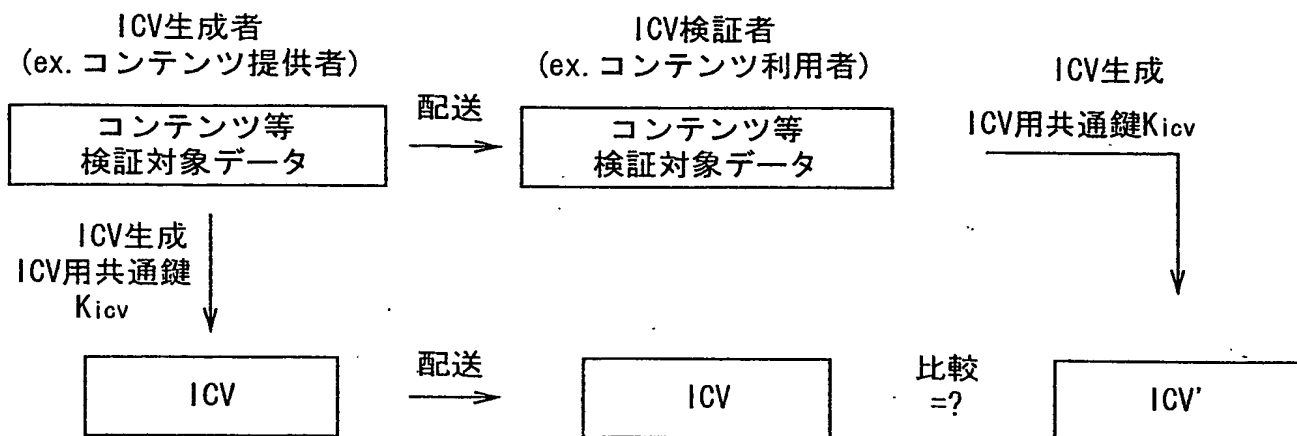


図 4 6

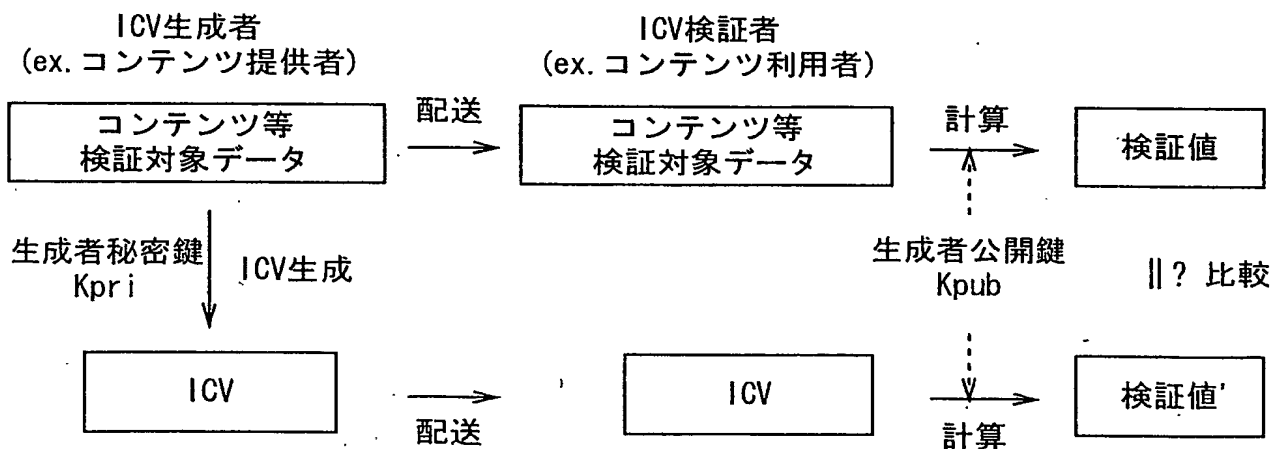


図 4 7

THIS PAGE BLANK (USPTO)

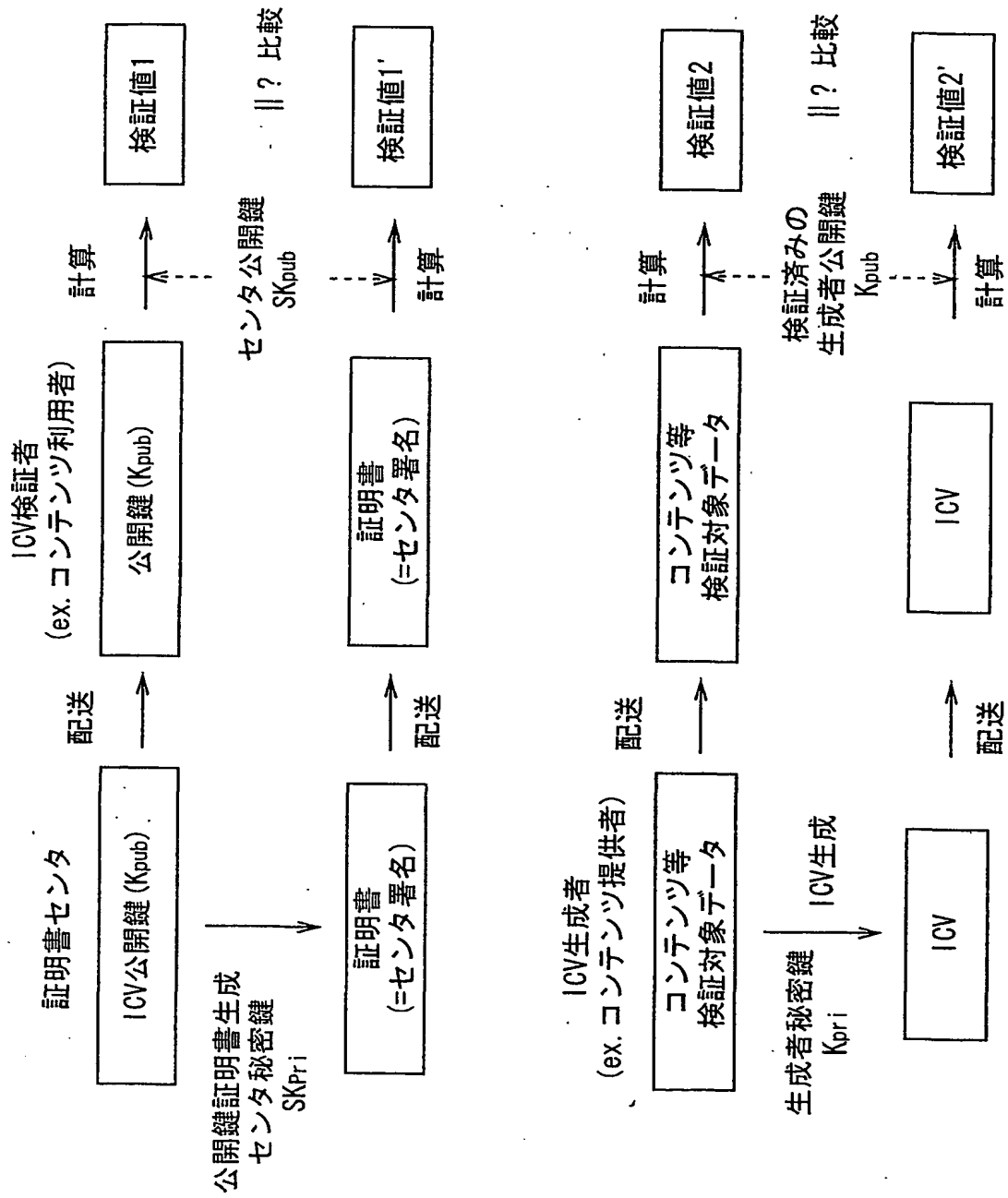


図 4 8

THIS PAGE BLANK (USTPO)

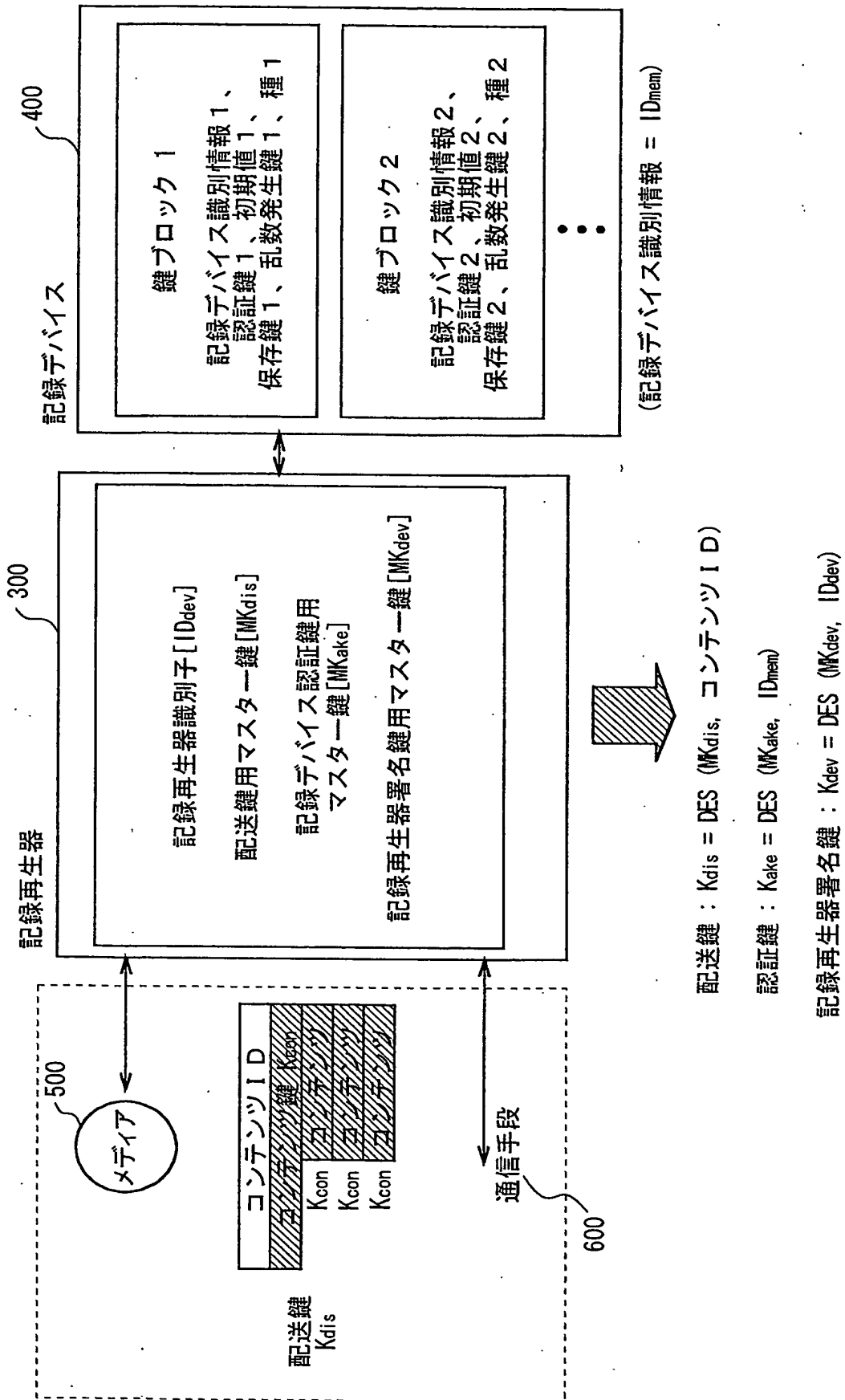


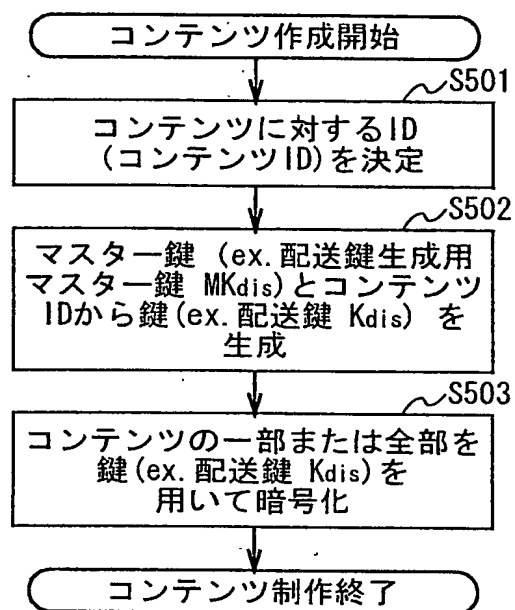
図 49

THIS PAGE BE BLANK (USPTO)

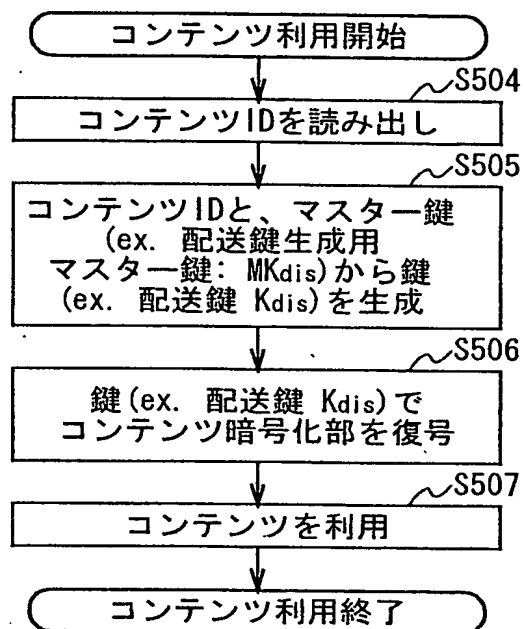
Master鍵から個別の鍵を生成する方法－(1)

[基本フロー]

コンテンツ制作または管理者

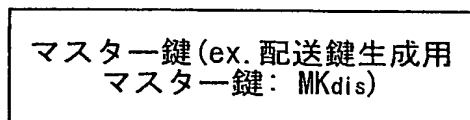


ユーザデバイス

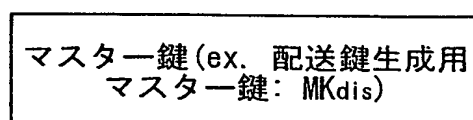


[鍵所有構成]

コンテンツ制作または管理者



ユーザデバイス



共有

コンテンツID

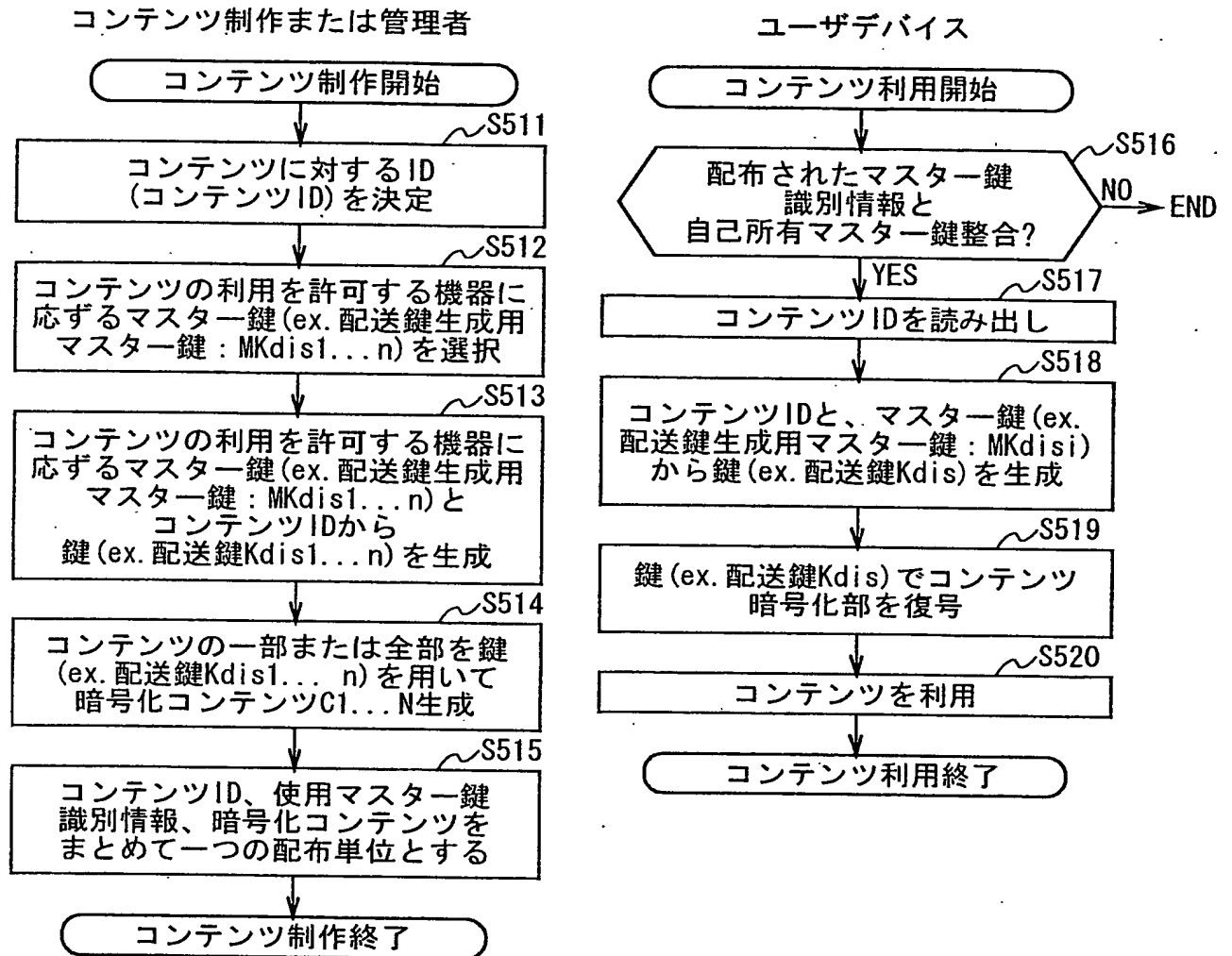
ID保護
コンテンツ

図 50

THIS PAGE BLANK (USPTO)

Master鍵から個別の鍵を生成する方法- (2)

[基本フロー]



[鍵所有構成]

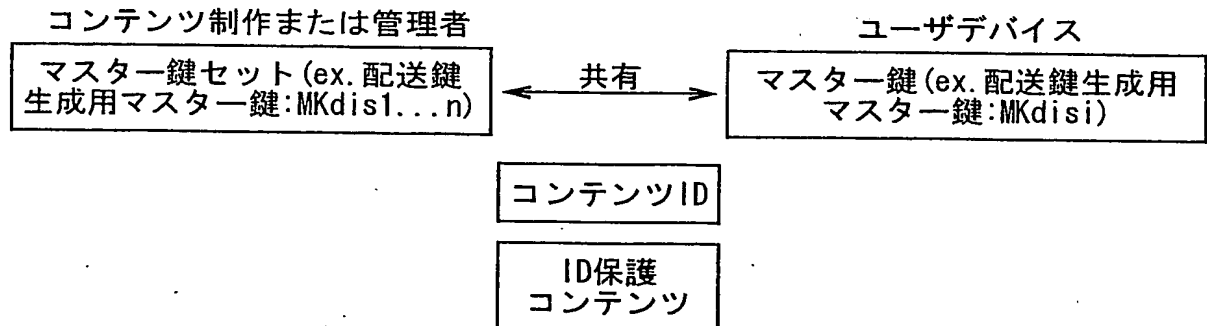


図 5 1

THIS PAGE BLANK (USPTO)

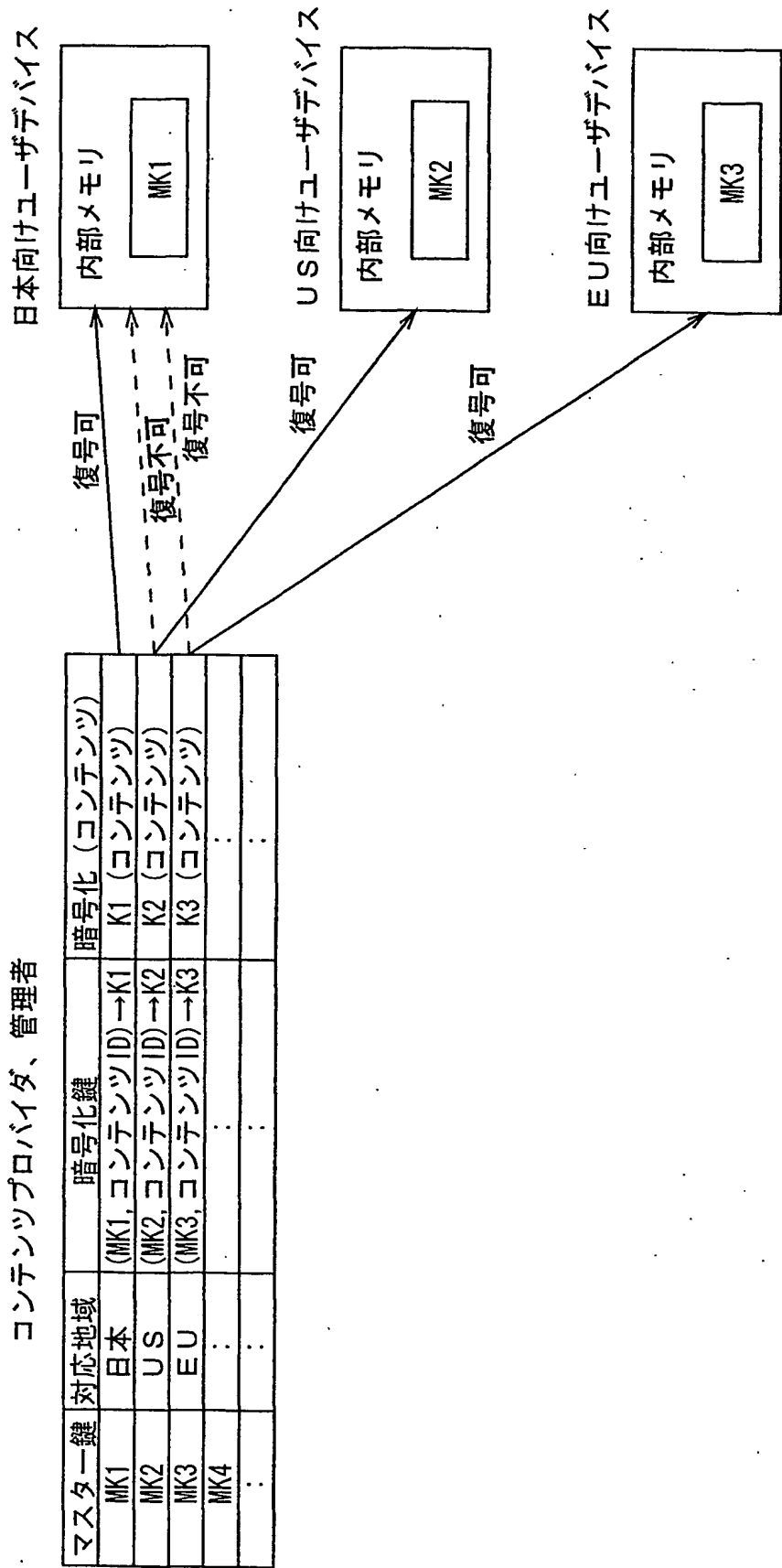


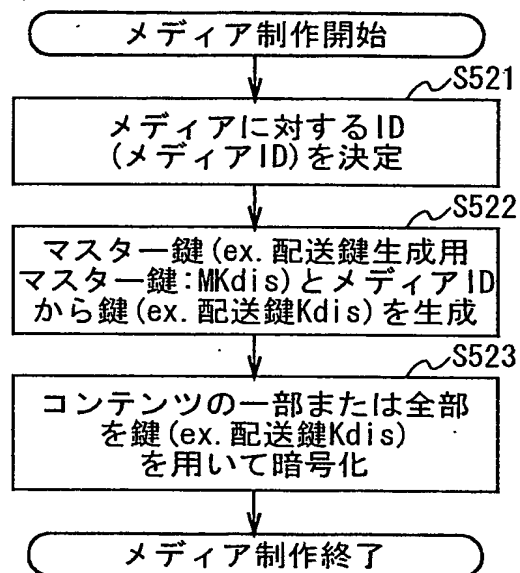
図 5 2

THIS PAGE BLANK (USPTO)

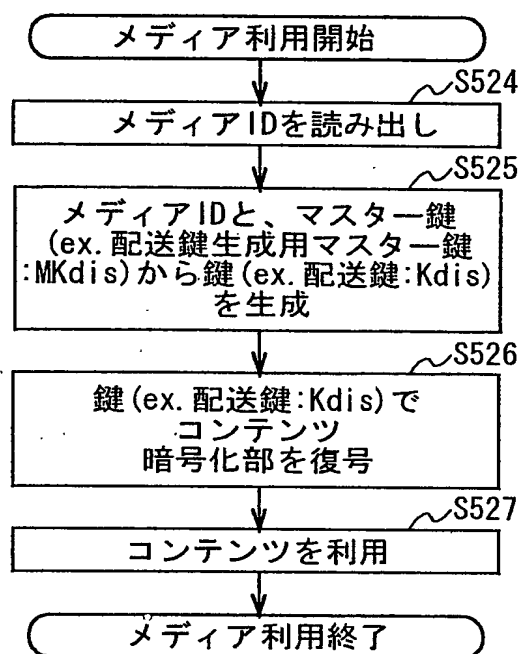
Master鍵から個別の鍵を生成する方法- (3)

[基本フロー]

メディア制作者または管理者

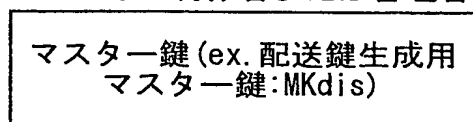


ユーザデバイス

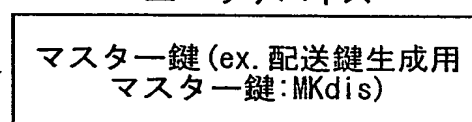


[鍵所有構成]

メディア制作者または管理者



ユーザデバイス



共有

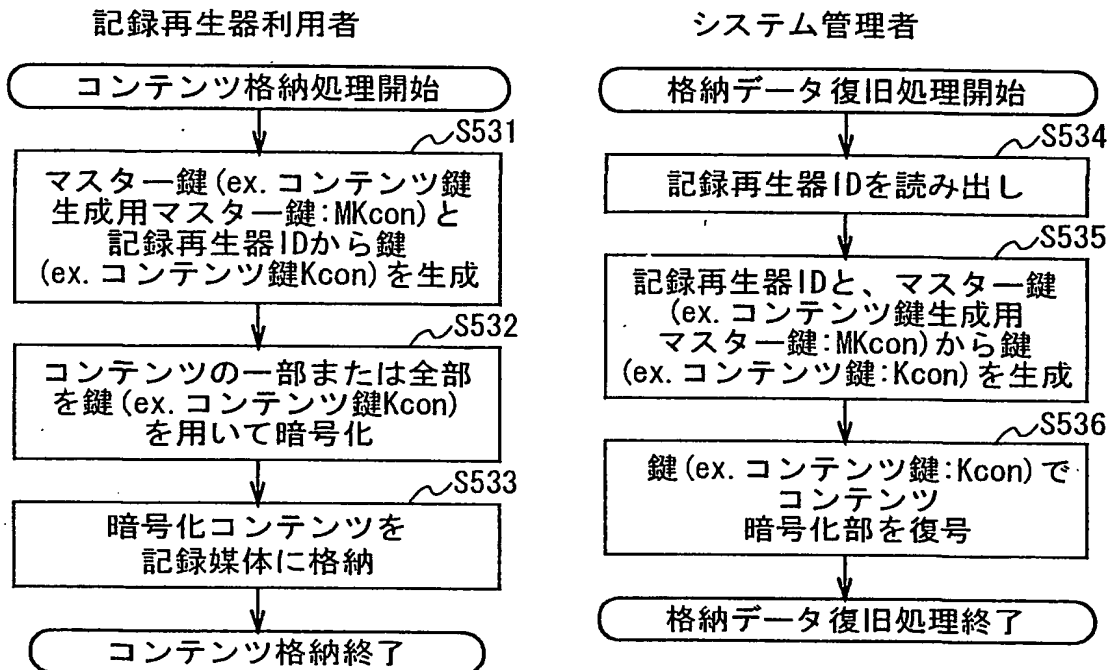


図 5 3

THIS PAGE BLANK (USPTO)

Master鍵から個別の鍵を生成する方法－(4)

[基本フロー]



[鍵所有構成]

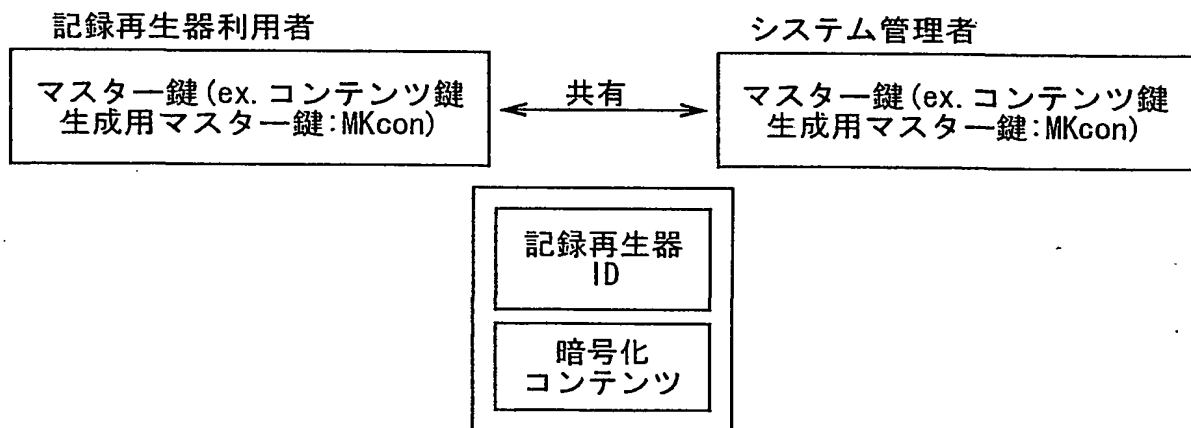
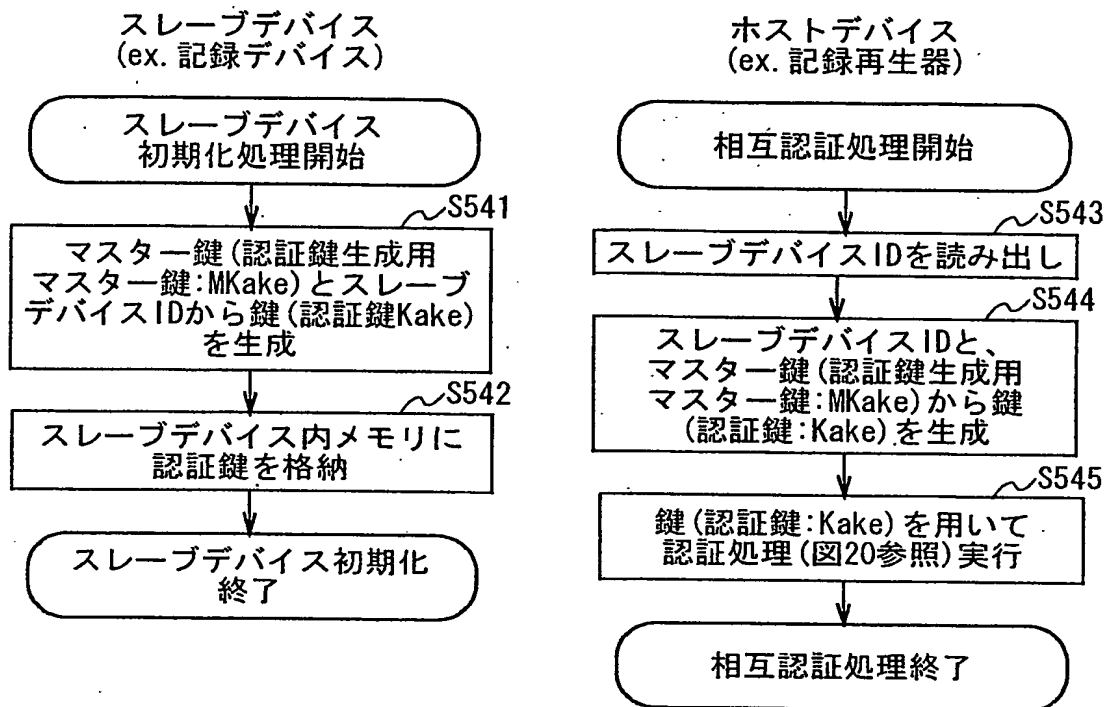


図 5 4

THIS PAGE BLANK (USPTO)

Master鍵から個別の鍵を生成する方法- (5)

[基本フロー]



[鍵所有構成]

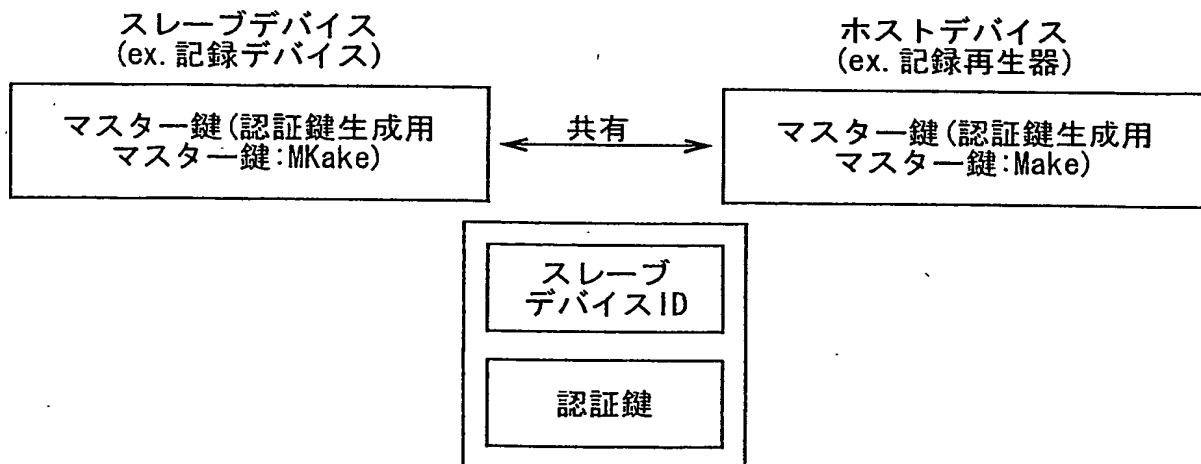


図 5 5

THIS PAGE BLANK (USPTO)

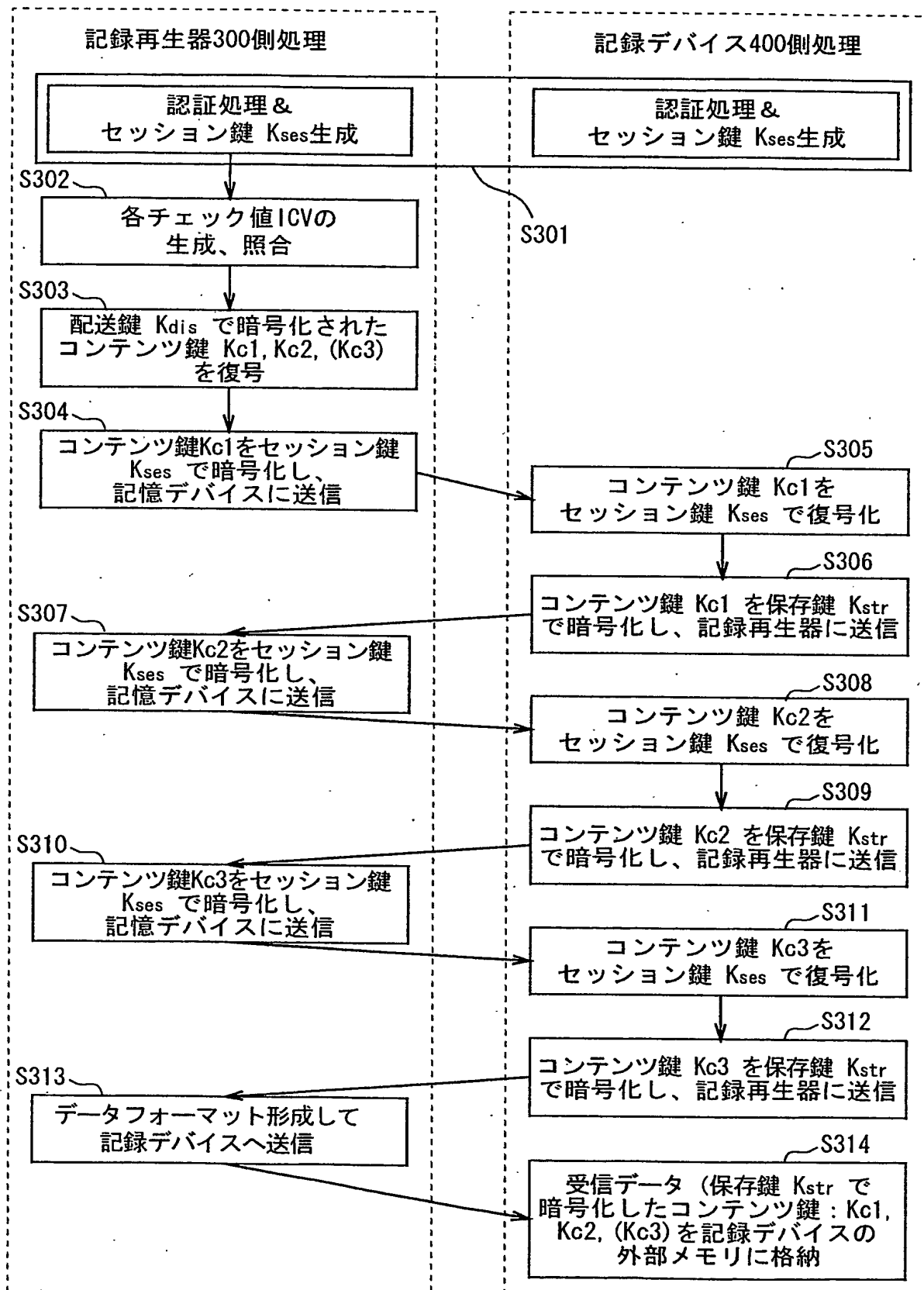
トリプルDESコンテンツ鍵: $Kc1, Kc2, (Kc3)$ の格納 (ダウンロード) 処理

図 5 6

THIS PAGE BLANK (USPTO)

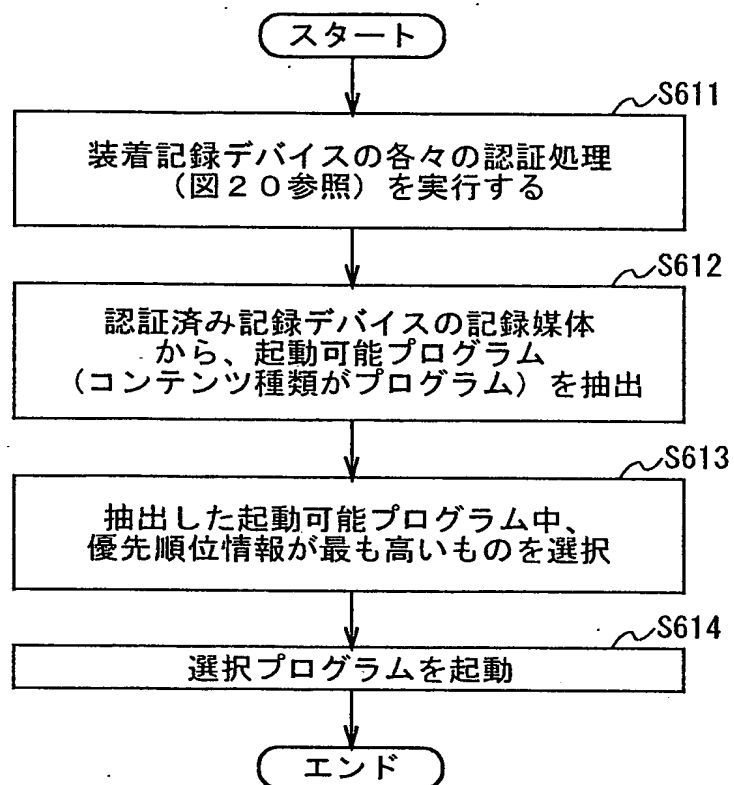


図57

THIS PAGE BLANK (USPTO)

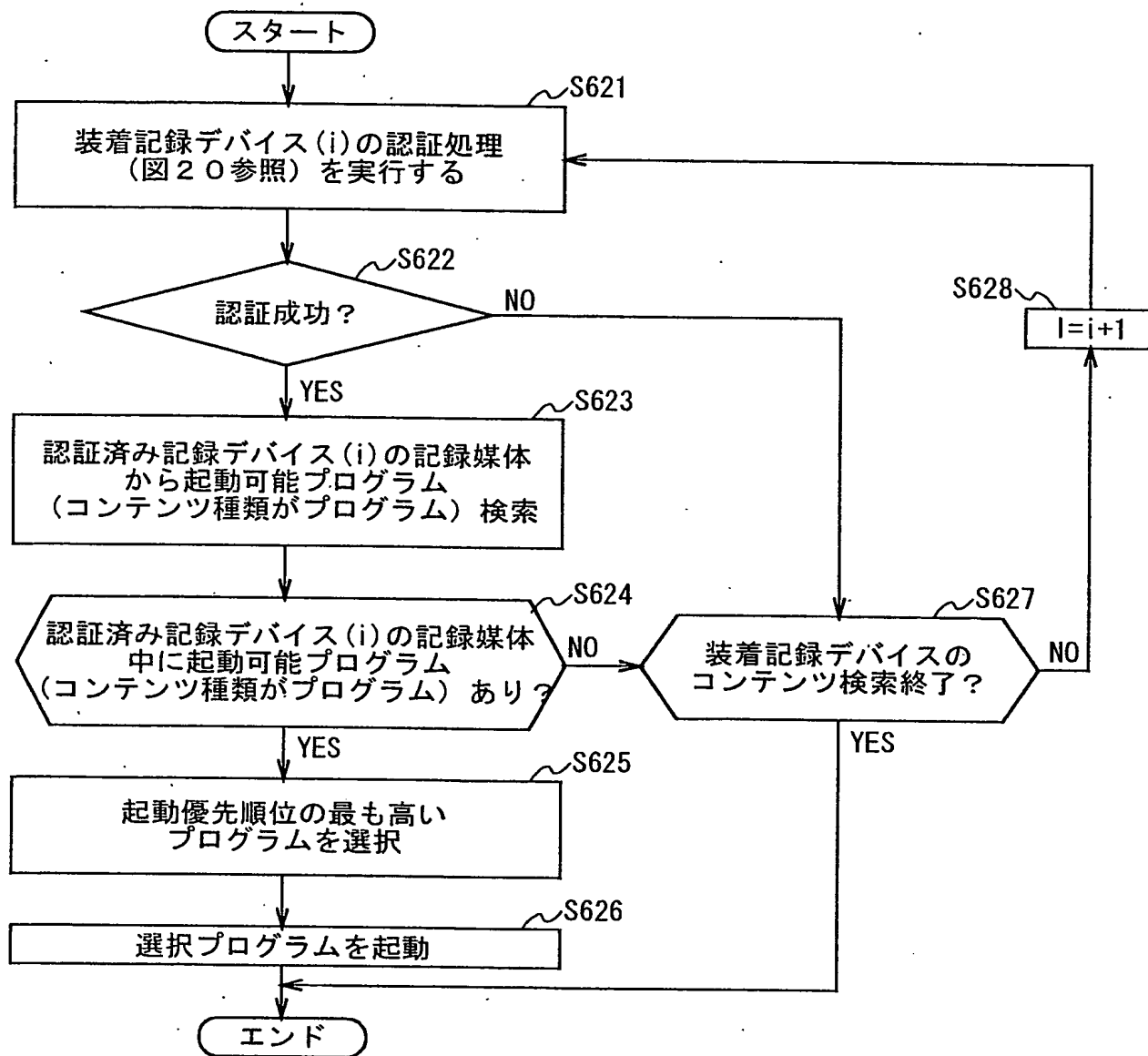


図 5 8

THIS PAGE BLANK (USPTO)

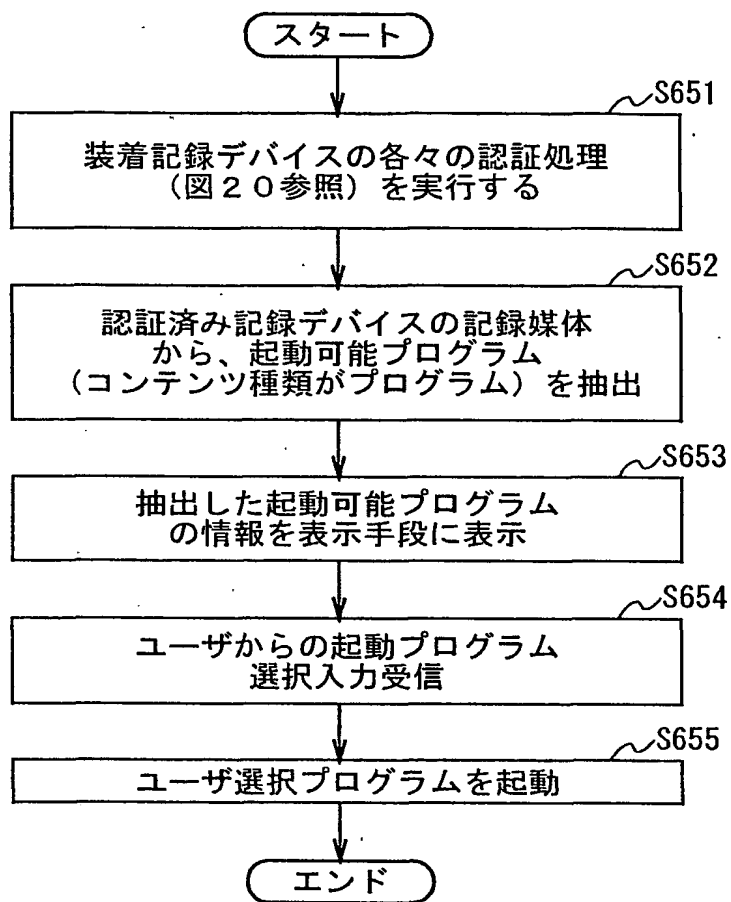


図59

THIS PAGE BLANK (USPTO)

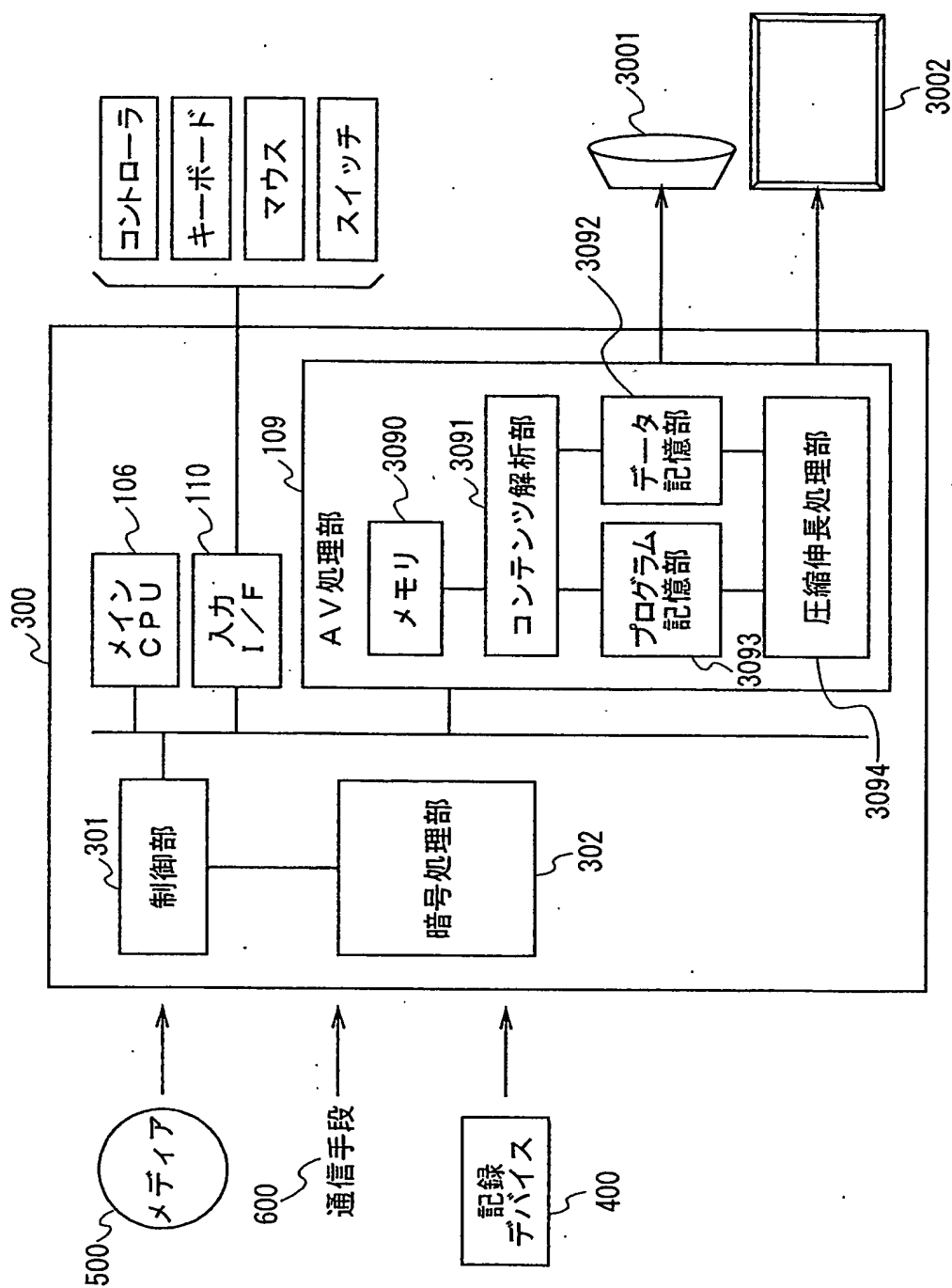


図 60

THIS PAGE BLANK (USPTO)

コンテンツ構成例 (1)

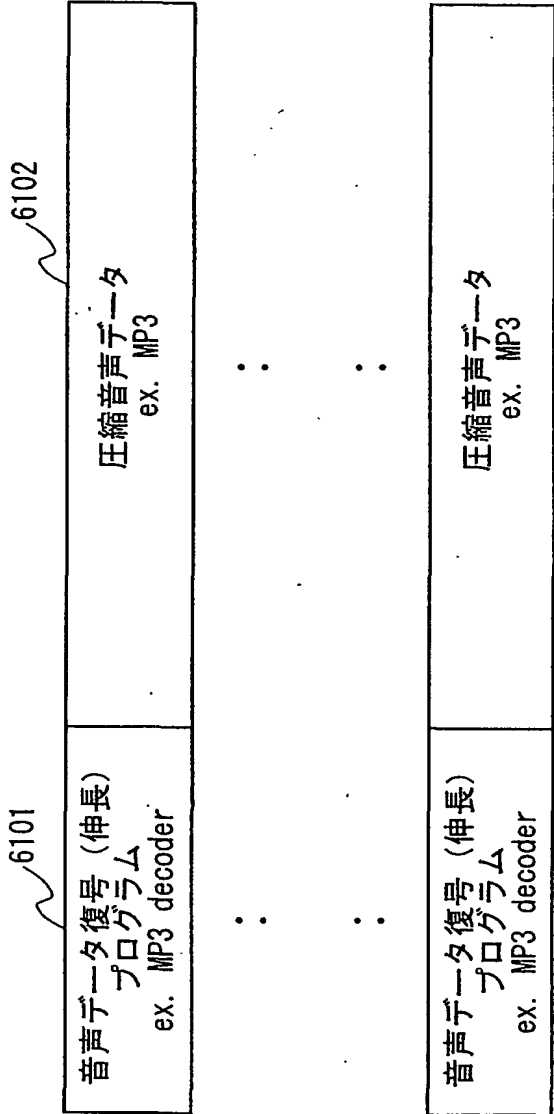


図 6 1

THIS PAGE BLANK (USPTO)

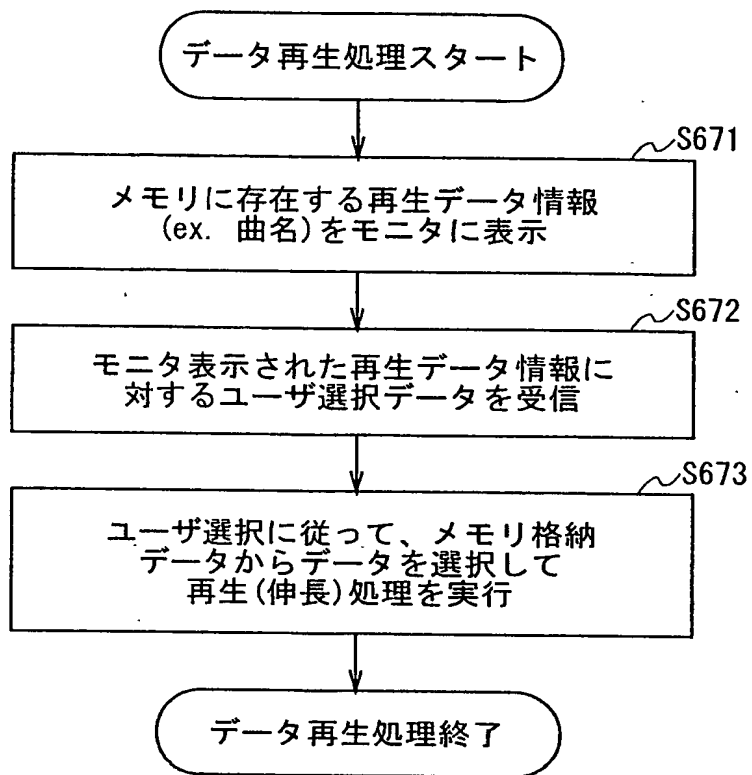


図 6 2

THIS PAGE BLANK (USPTO)

コンテンツ構成例 (2)

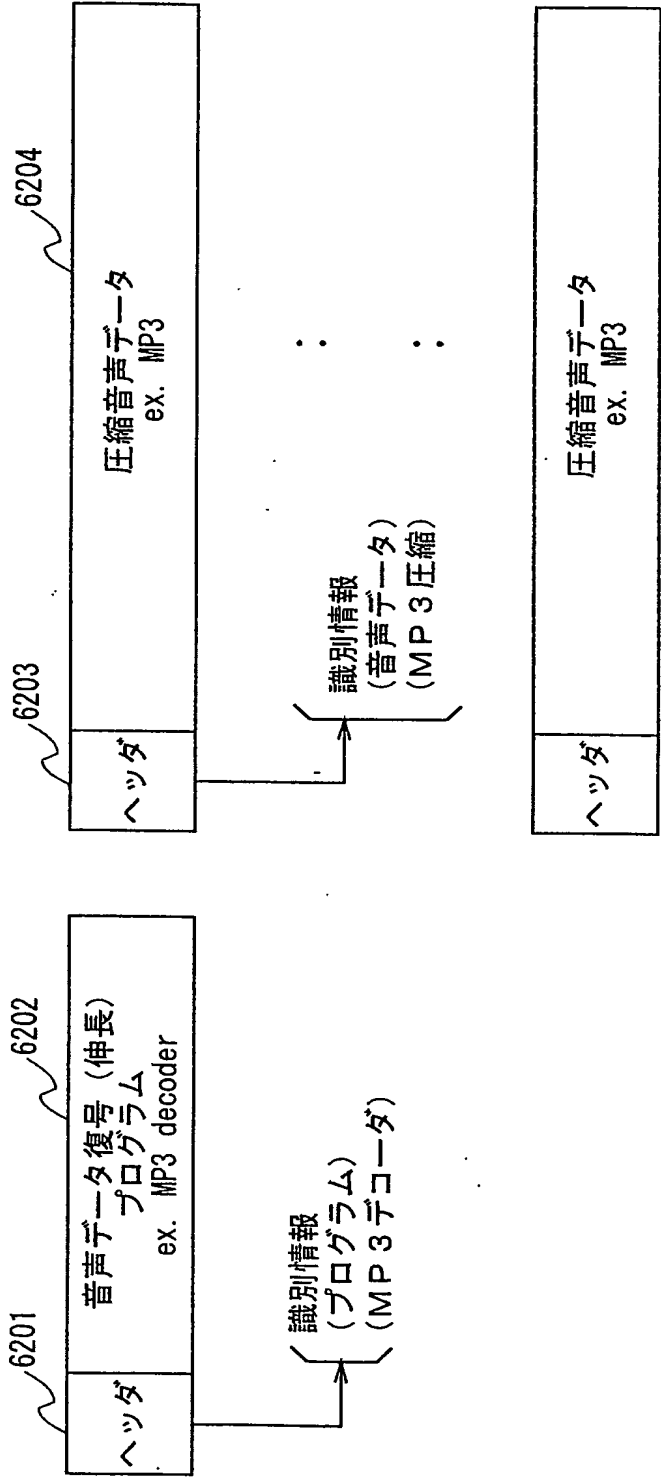


図 6 3

THIS PAGE BLANK (uspto)

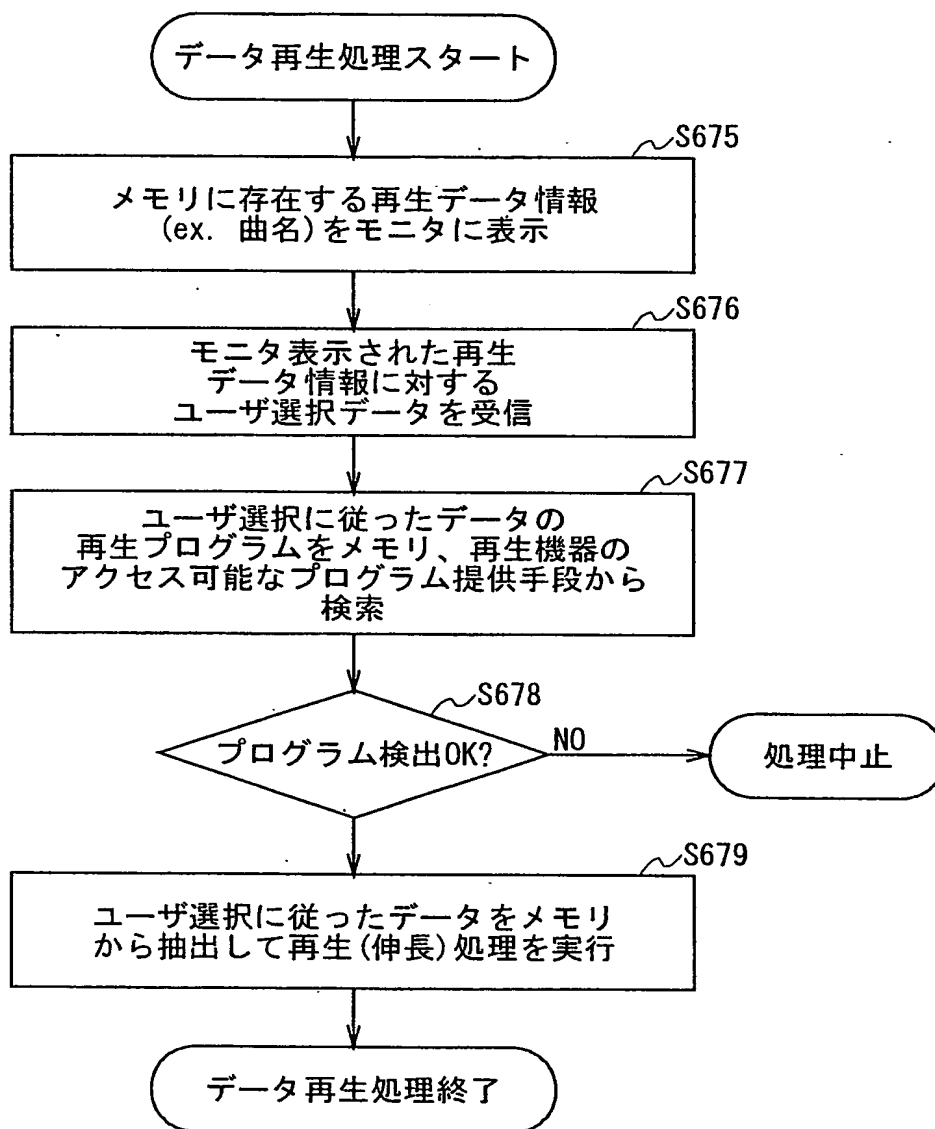


図 6 4

THIS PAGE BLANK (USPS)

コンテンツ構成例 (3)

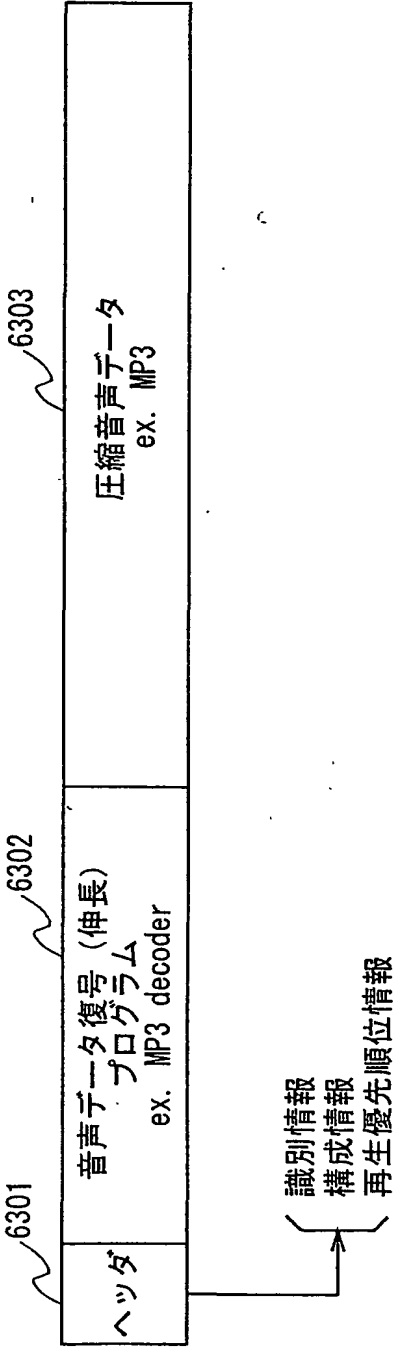


図 6 5

THIS PAGE BLANK (0151910)

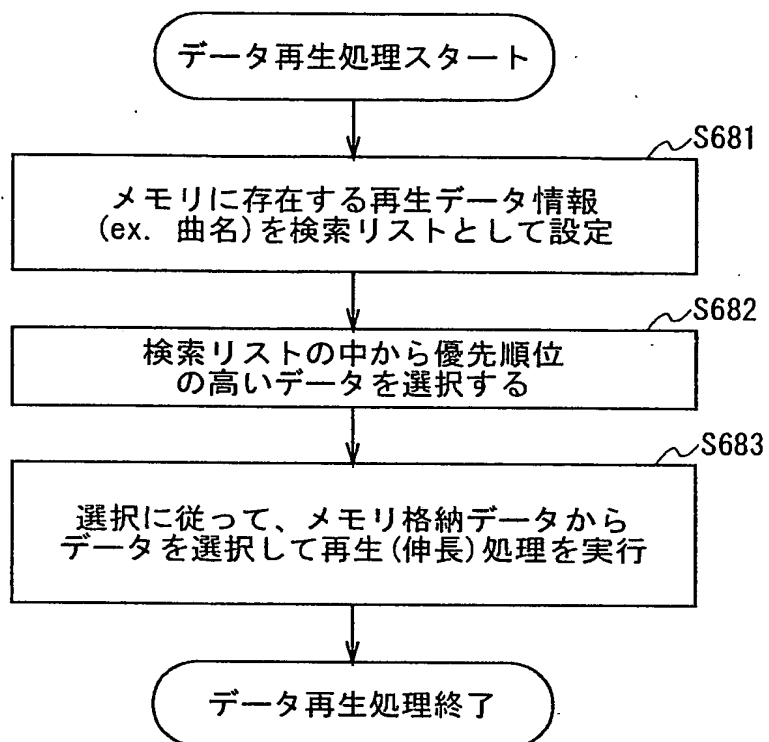


図 6 6

THIS PAGE BLANK (USPTO)

コンテンツ構成例 (4)

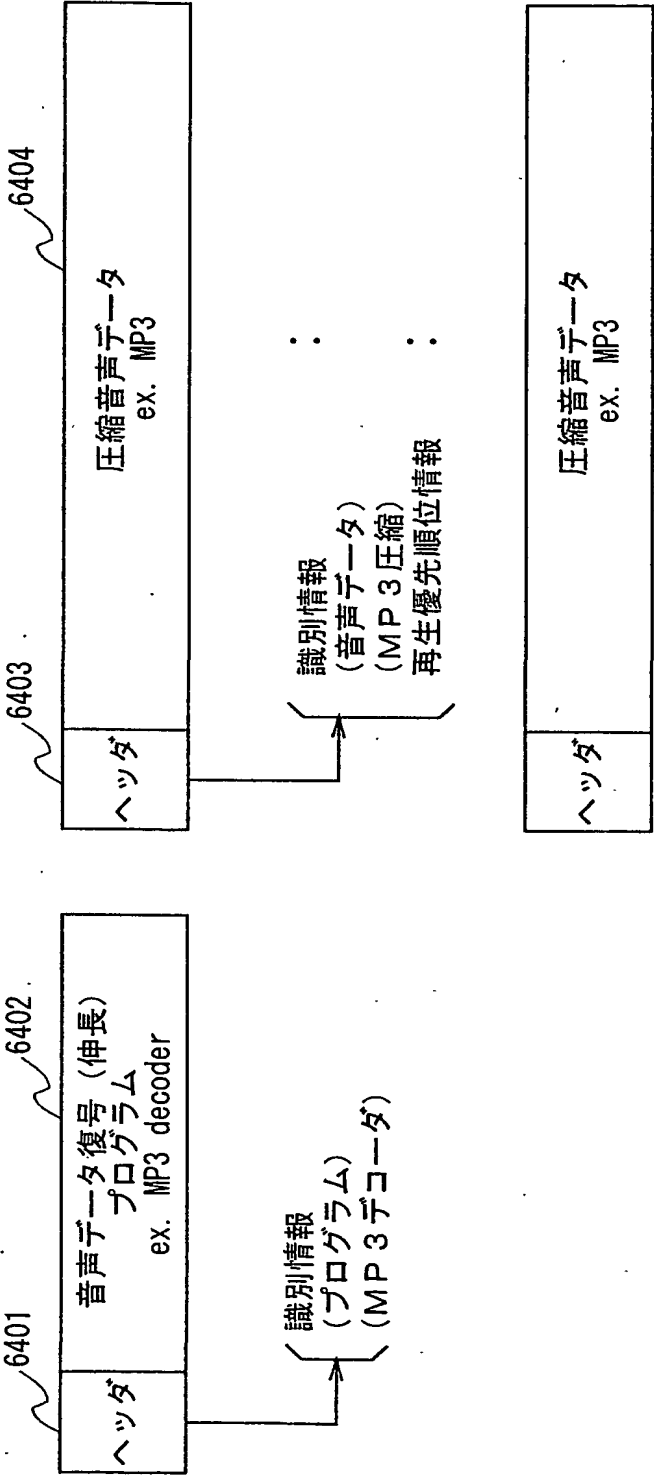


図 67

THIS PAGE BLANK (USPTO)

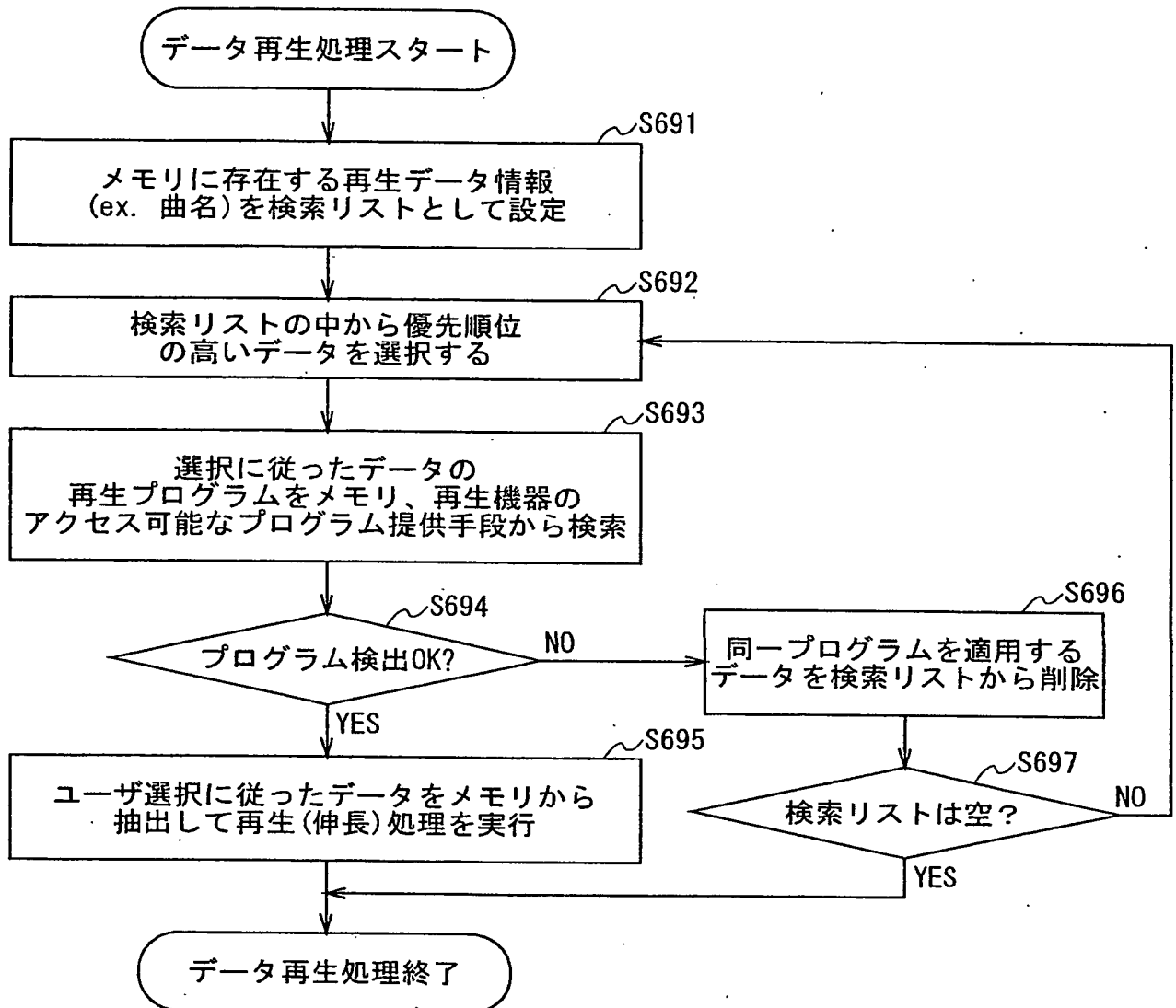


図 6 8

THIS PAGE BLANK (USPTO)

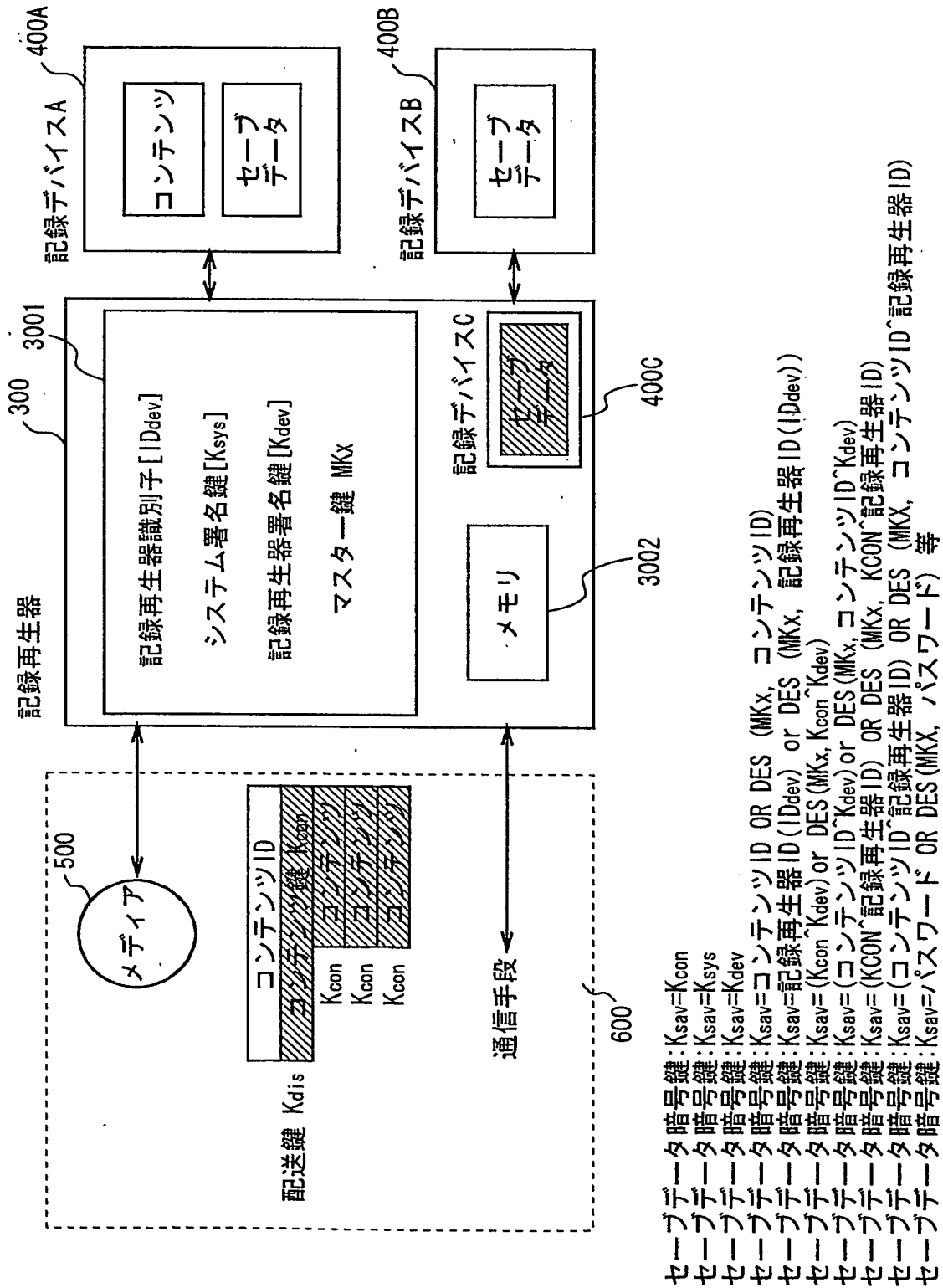


図 6 9

THIS PAGE BLANK (USPTO)

(1) コンテンツ固有鍵、or システム共通鍵を使用したセーブデータ格納処理例

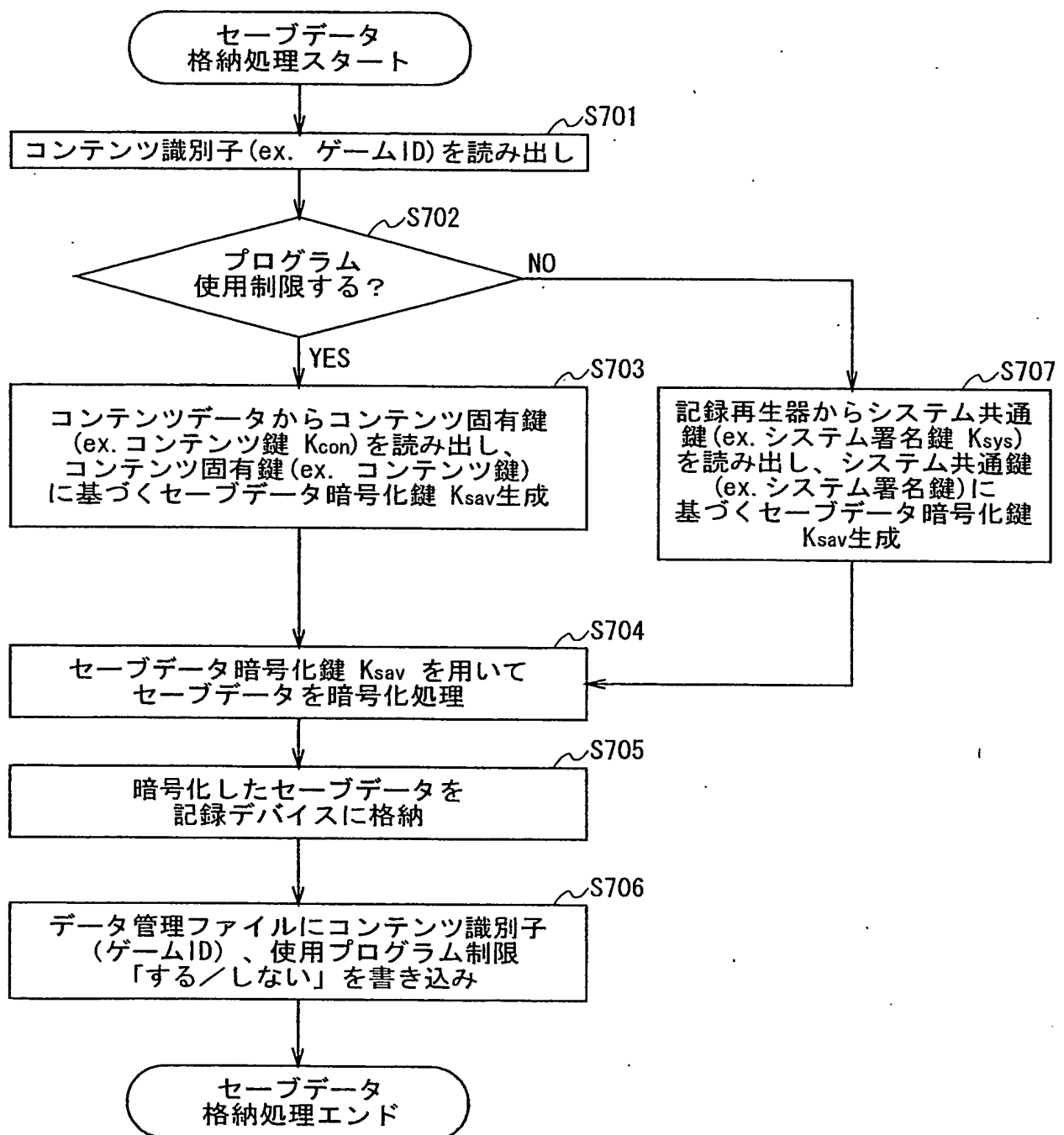


図 70

THIS PAGE BLANK (USTPO)

データ管理ファイル (1)

データ 番号	コンテンツ識別子 (ゲーム I D)	記録再生器識別子 (I D dev)	プログラム 使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	しない
⋮	⋮	⋮	⋮

図 7 1

THIS PAGE BLANK (USPTO)

(2) コンテンツ固有鍵、or システム共通鍵を使用したセーブデータ再生処理例

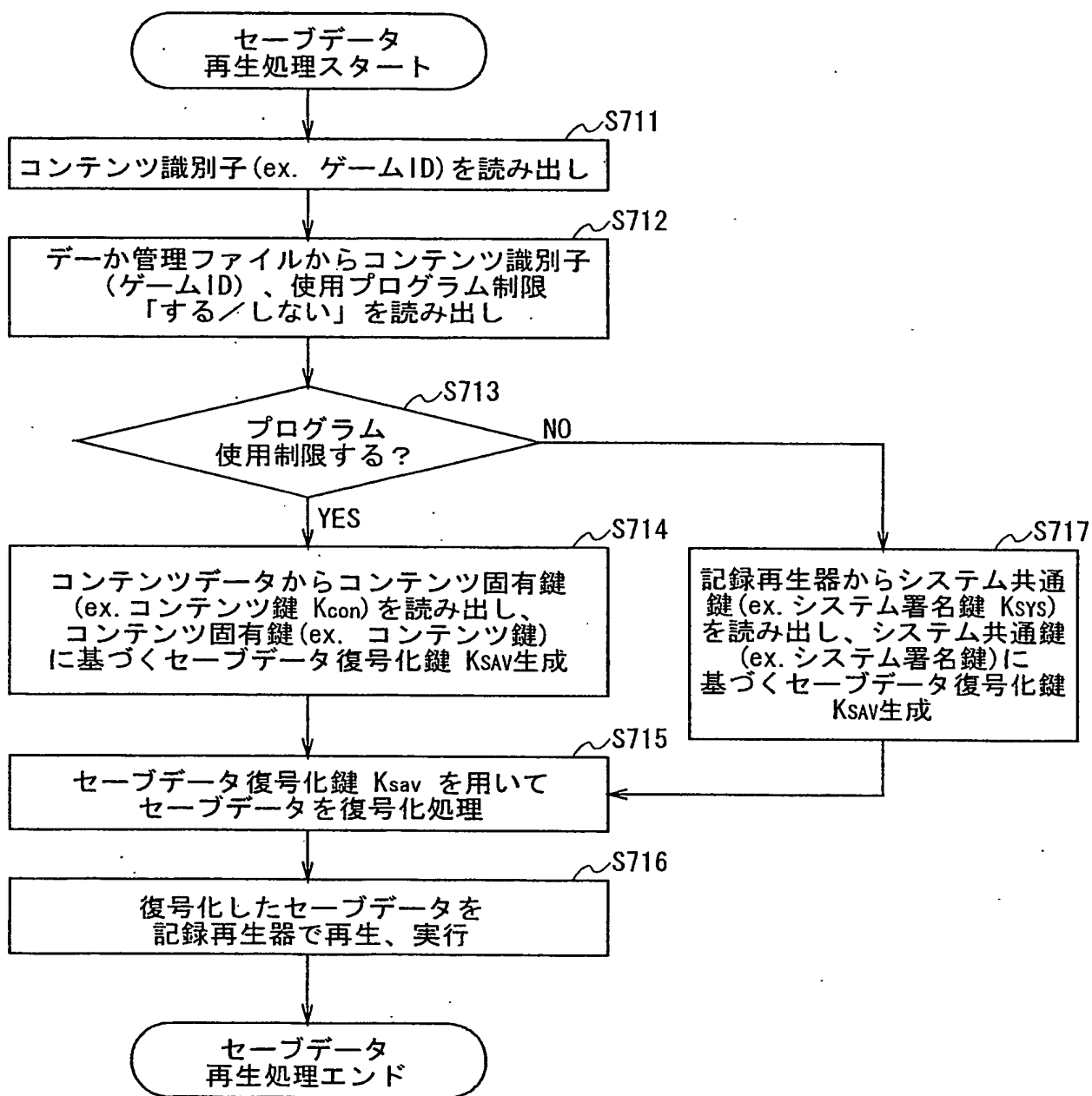


図 7 2

THIS PAGE BLANK (uspto)

(3) コンテンツID、or システム共通鍵を使用したセーブデータ格納処理例

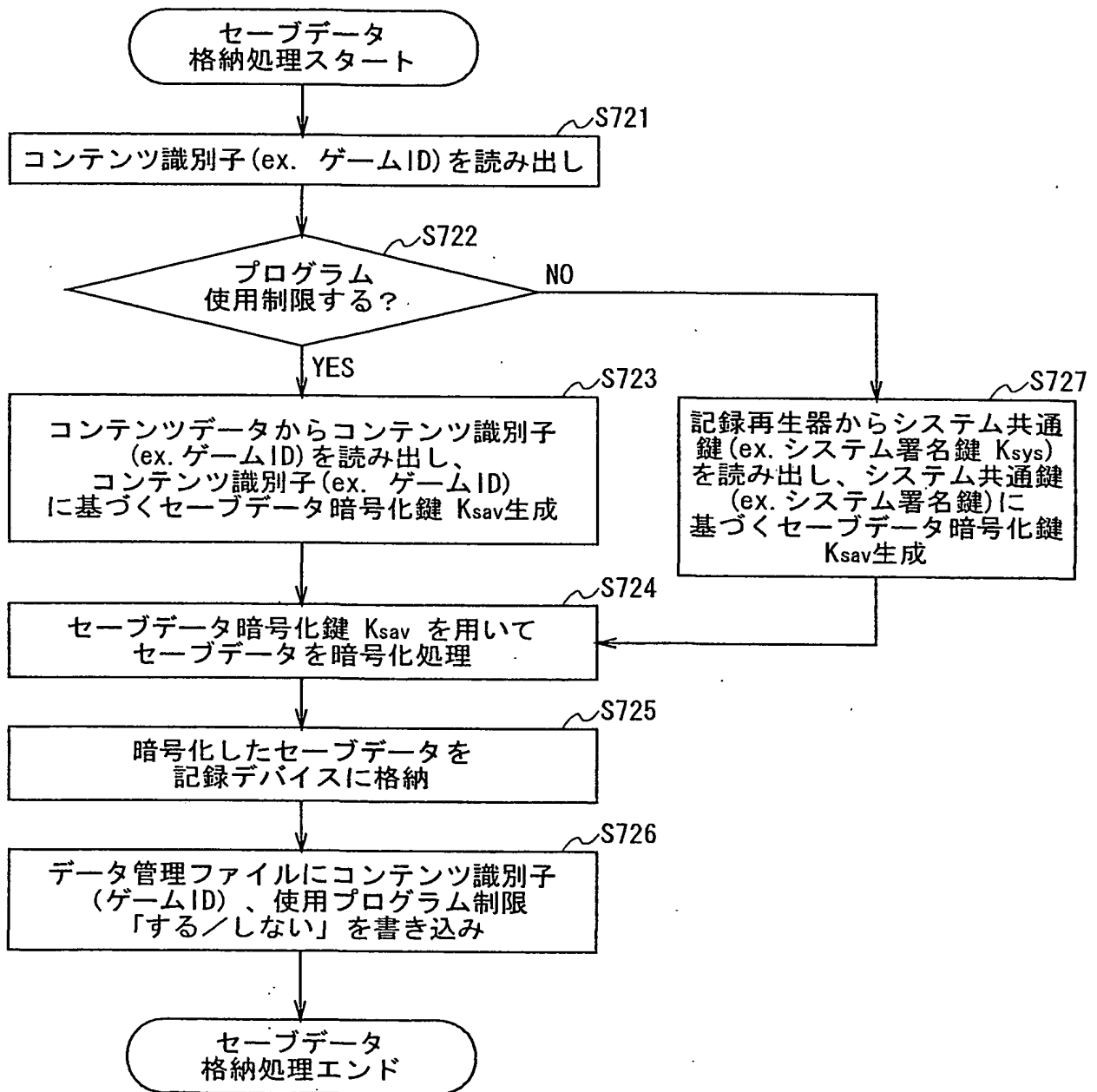


図 7 3

THIS PAGE BEGINS BLANK (USPTO)

(4) コンテンツID、or システム共通鍵を使用したセーブデータ再生処理例

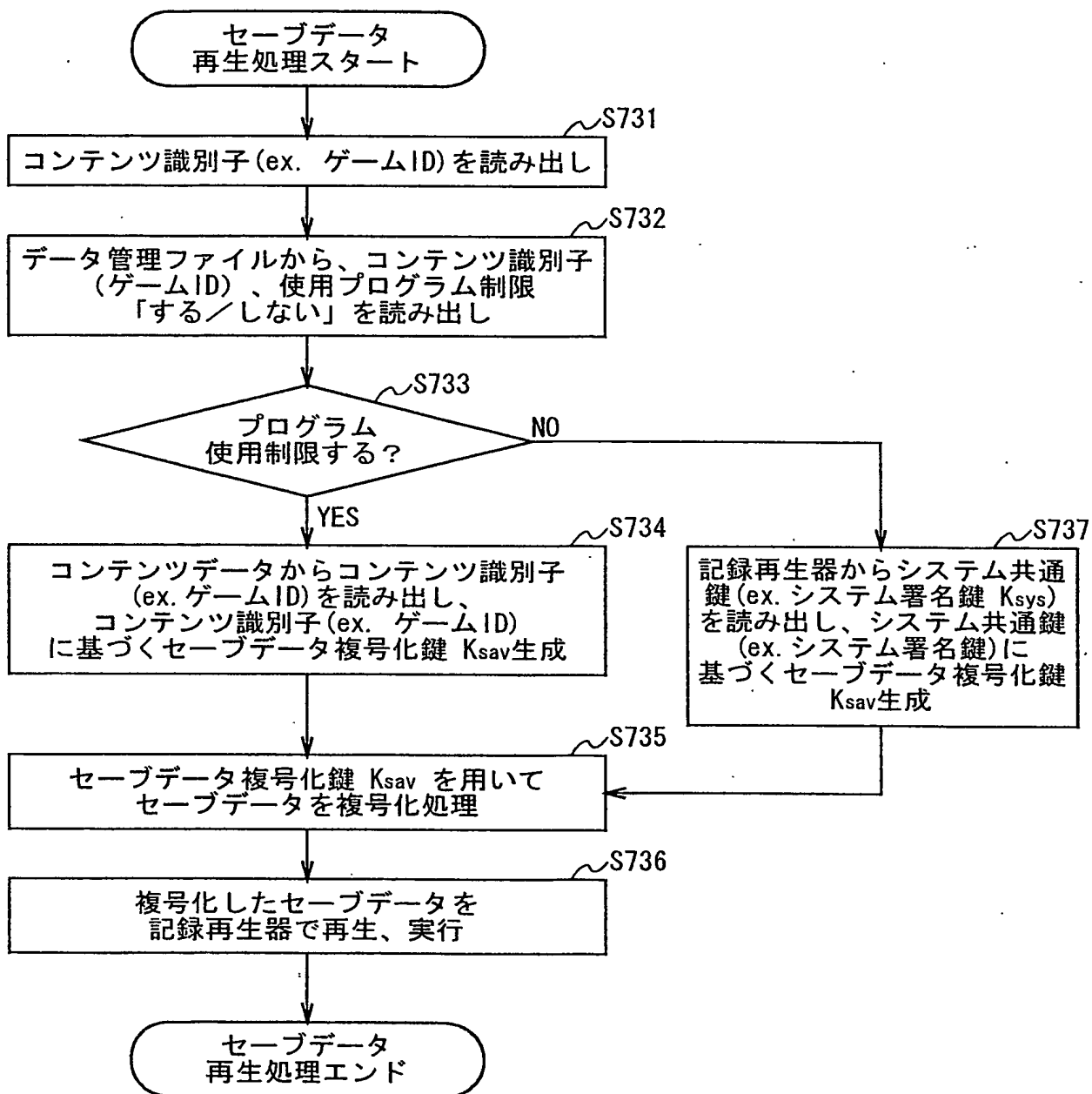


図 7 4

THIS PAGE BLANK (USPTO)

(5) 記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例

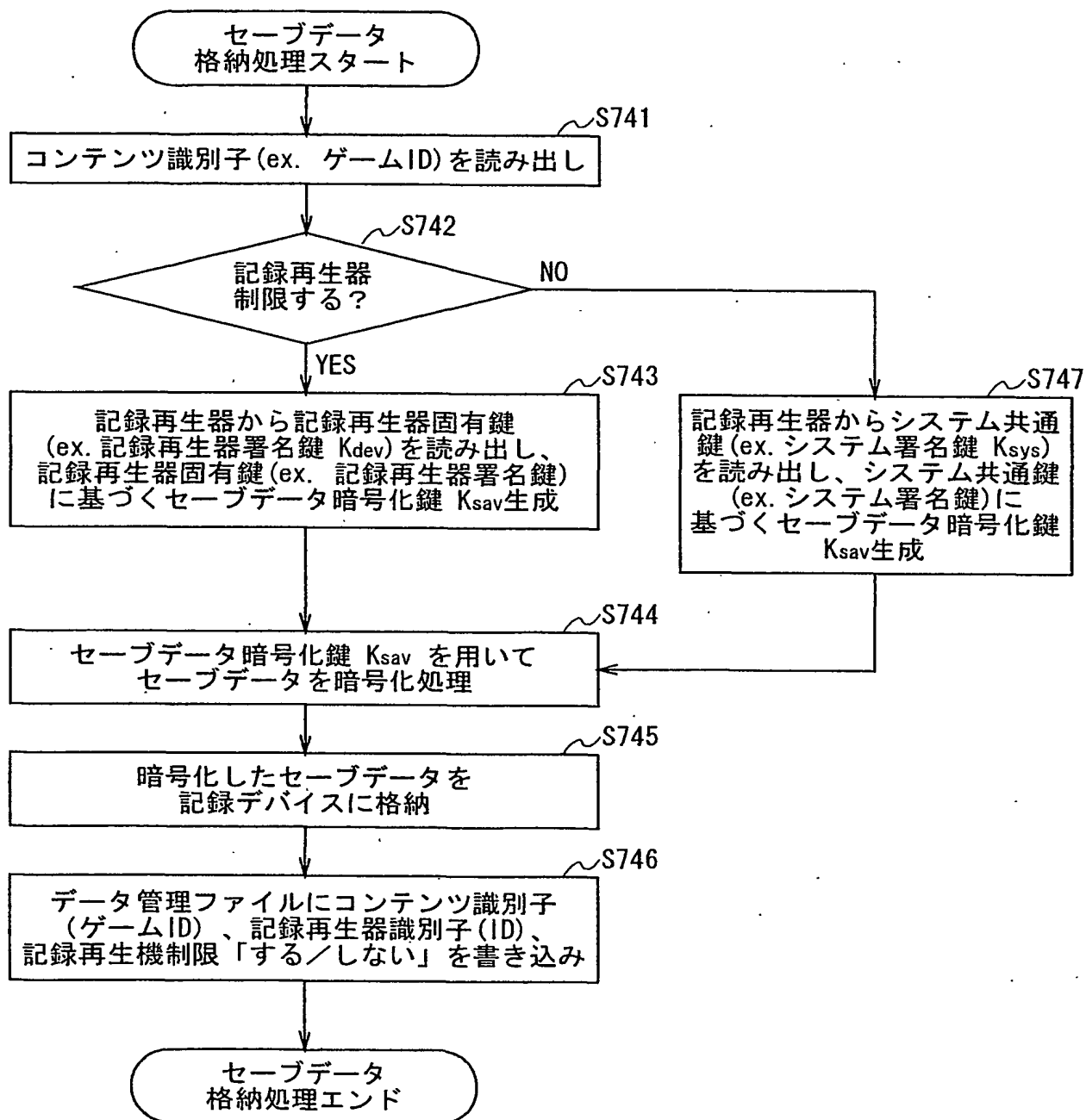


図 7 5

THIS PAGE BLANK (user)

データ管理ファイル (2)

データ 番号	コンテンツ識別子 (ゲーム I D)	記録再生器識別子 (I D dev)	記録再生器 制限
1	12345678...	56789012...	しない
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	する
⋮	⋮	⋮	⋮

図 7 6

THIS PAGE BLANK (ustp10)

(6) 記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例

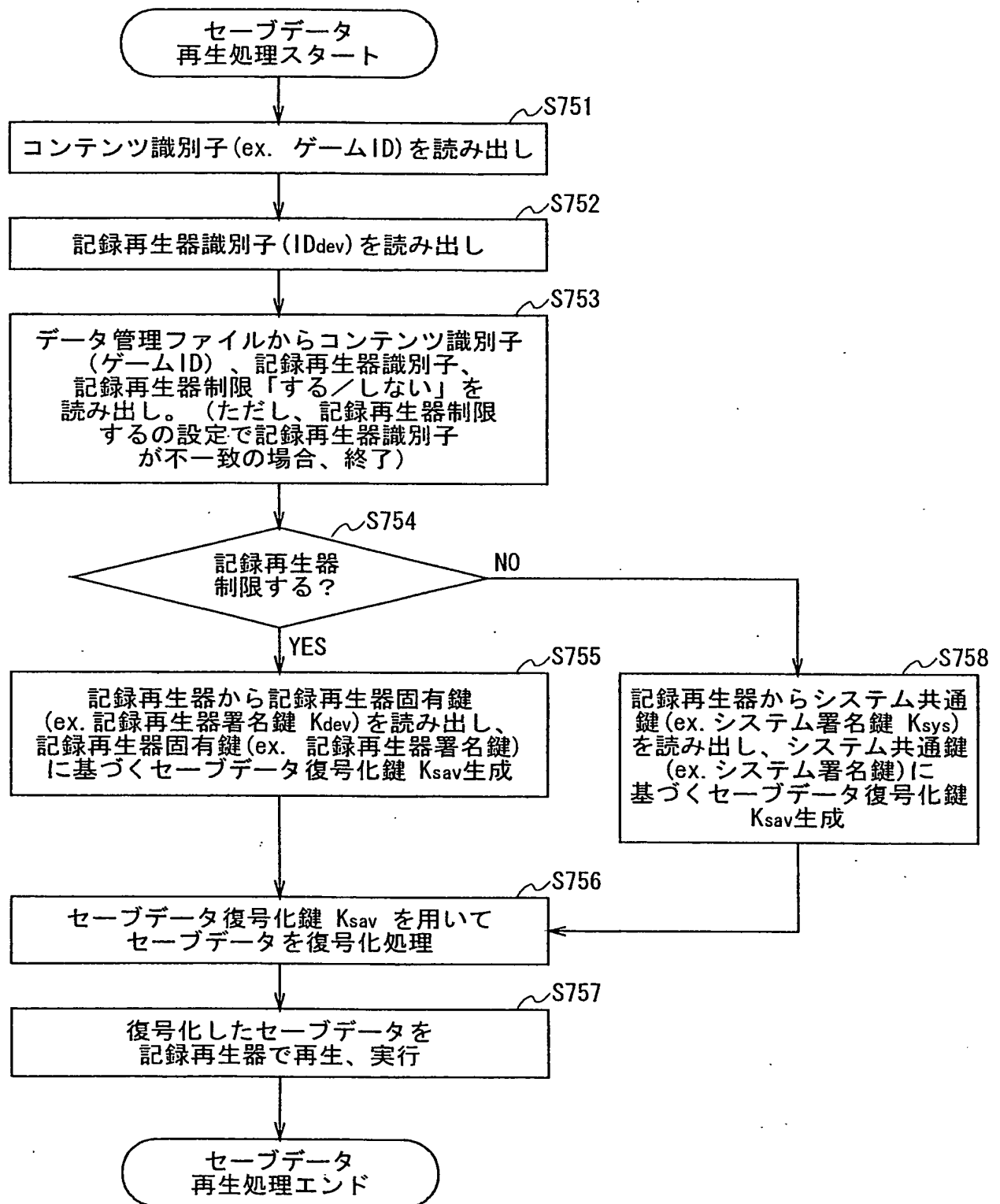


図 7 7

THIS PAGE BLANK (USPS)

(7) 記録再生器識別子、or システム共通鍵を使用したセーブデータ格納処理例

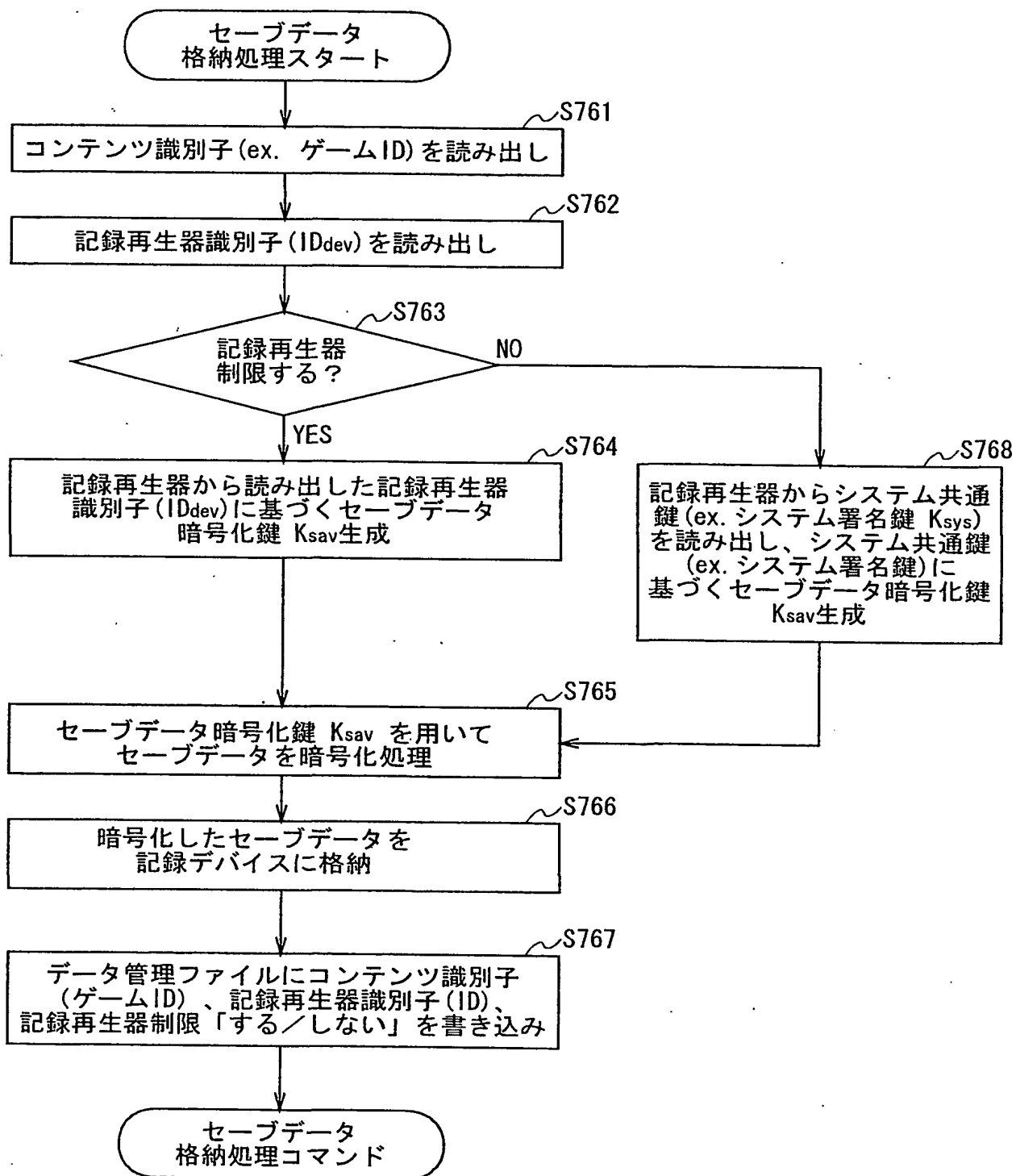
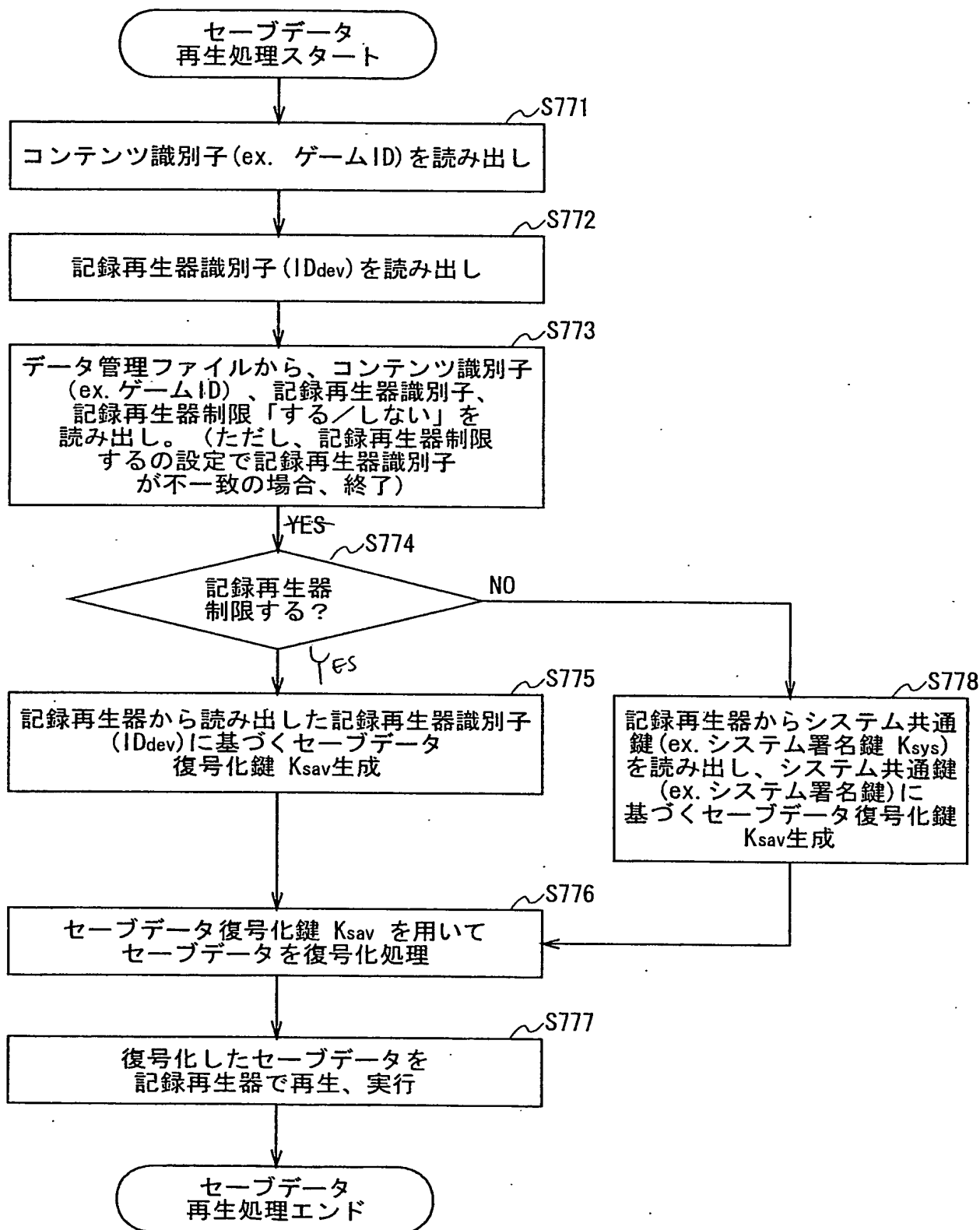


図 7 8

THIS PAGE BLANK (USPTO)

(8) 記録再生器識別子、or システム共通鍵を使用したセーブデータ再生処理例



THIS PAGE IS BLANK (user)

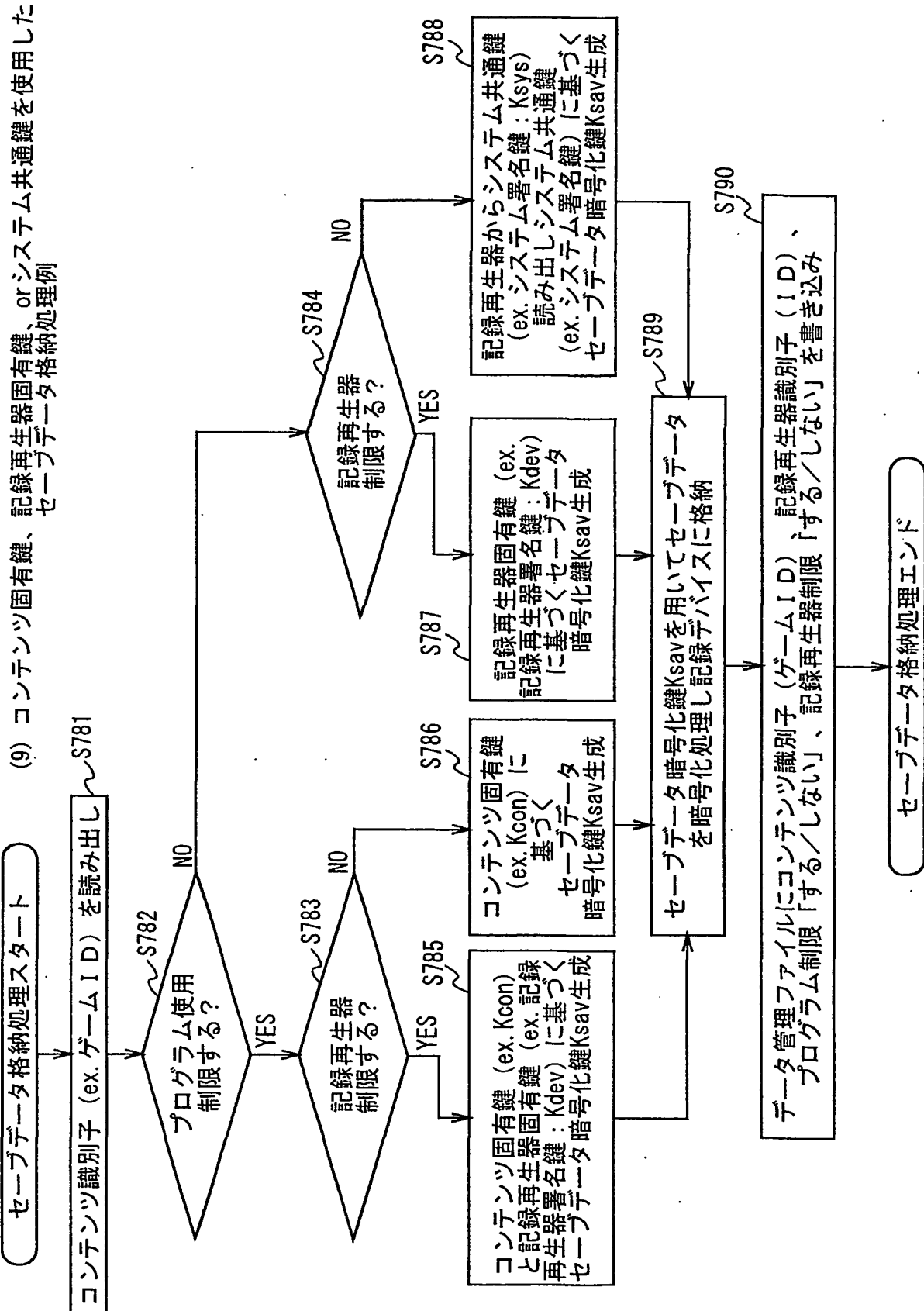


図 80

THIS PAGE BLANK (USPTO)

データ管理ファイル (3)

データ 番号	コンテンツ識別子 (ゲーム I D)	記録再生器識別子 (I D dev)	プログラム 使用制限	記録再生器 制限
1	12345678...	56789012...	する	しない
2	ABCDEF12...	09876543...	する	する
3	12245678...	58834762...	しない	する
⋮	⋮	⋮	⋮	⋮

図 8 1

THIS PAGE BLANK (USPS10)

セーブデータ再生処理スタート
(10) コンテンツ固有鍵、記録再生装置固有鍵、
or システム共通鍵を使用したセーブデータ再生処理例

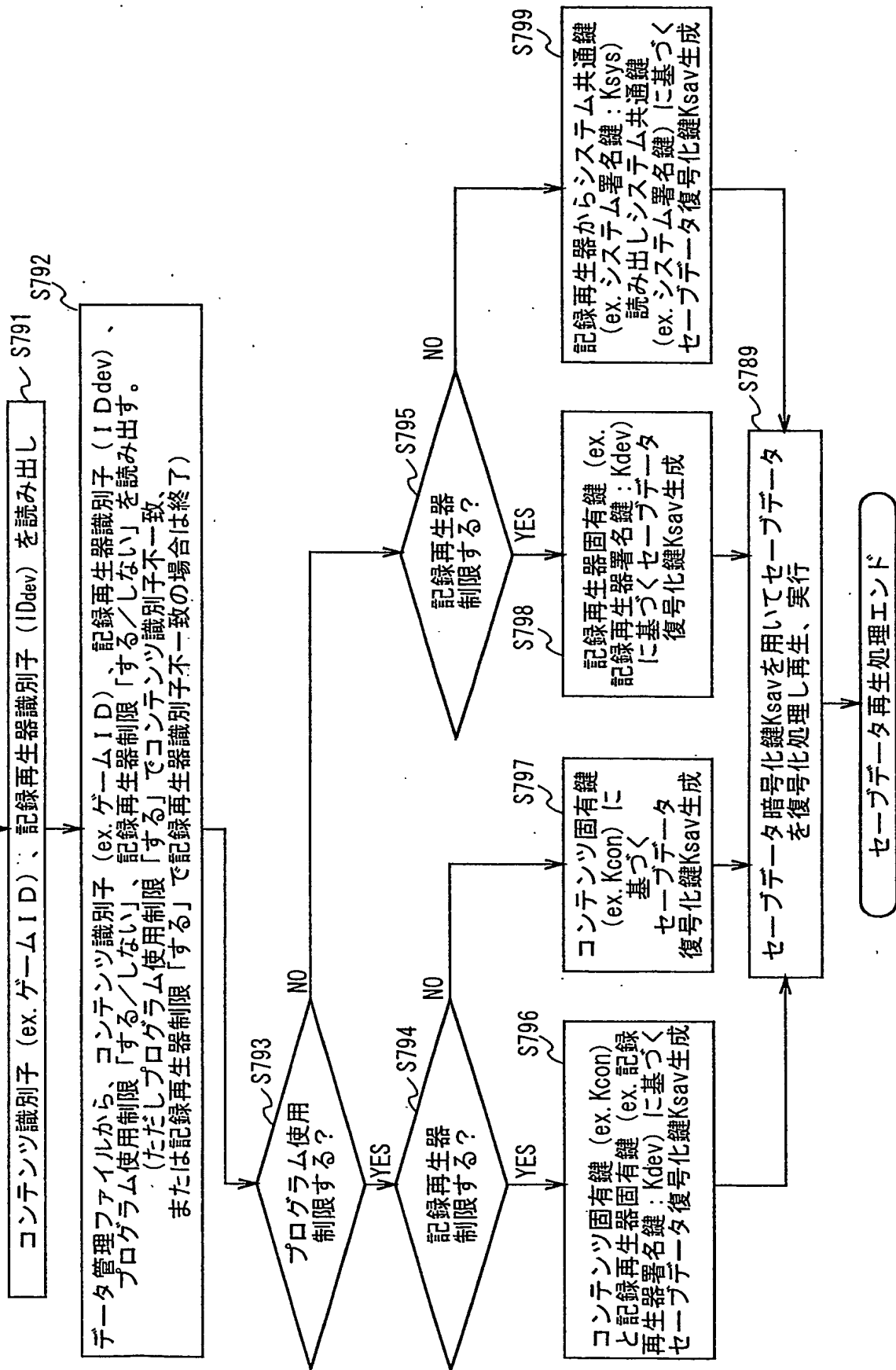


図 8 2

THIS PAGE BLANK (USPSTO)

(11) ユーザパスワード、or システム共通鍵を使用したセーブデータ格納処理例

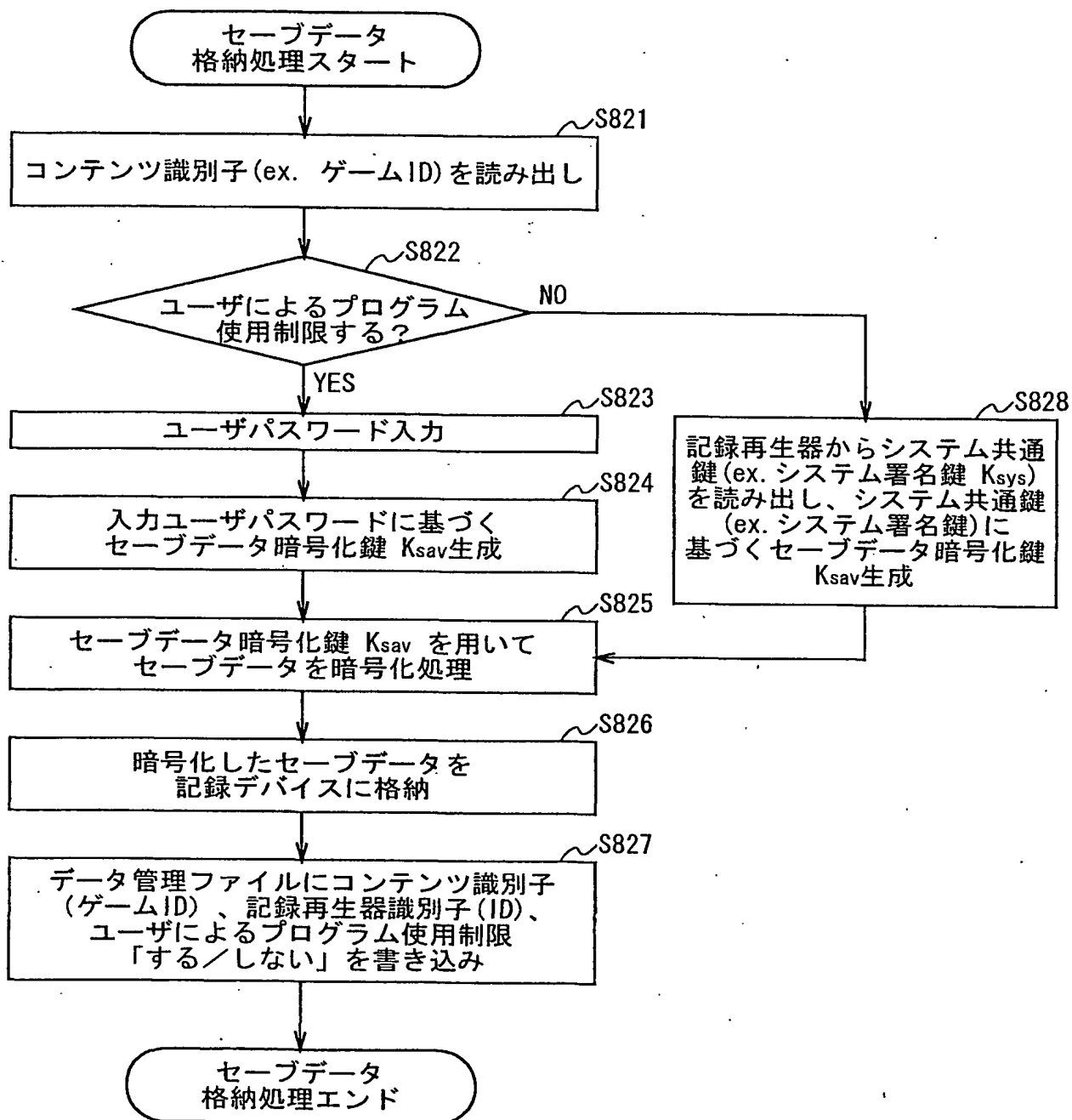


図 8 3

THIS PAGE BLANK (USPTO)

データ管理ファイル (4)

データ 番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (IDdev)	ユーザによる プログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	しない
⋮	⋮	⋮	⋮

図 8 4

THIS PAGE BLANK (U) (S) (P)

(12) ユーザパスワード、or システム共通鍵を使用したセーブデータ再生処理例

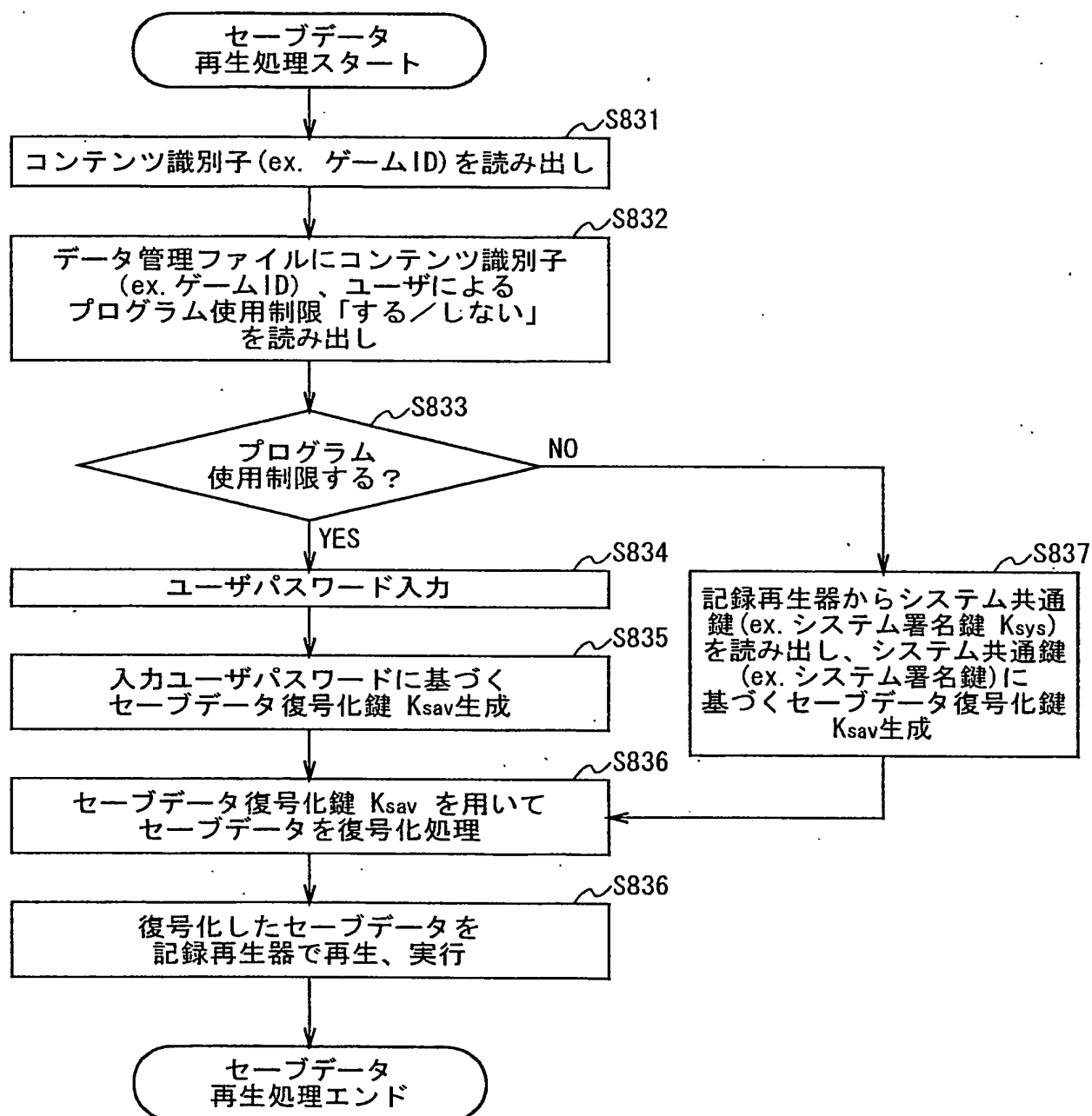


図 8 5

THIS PAGE BLANK (user)

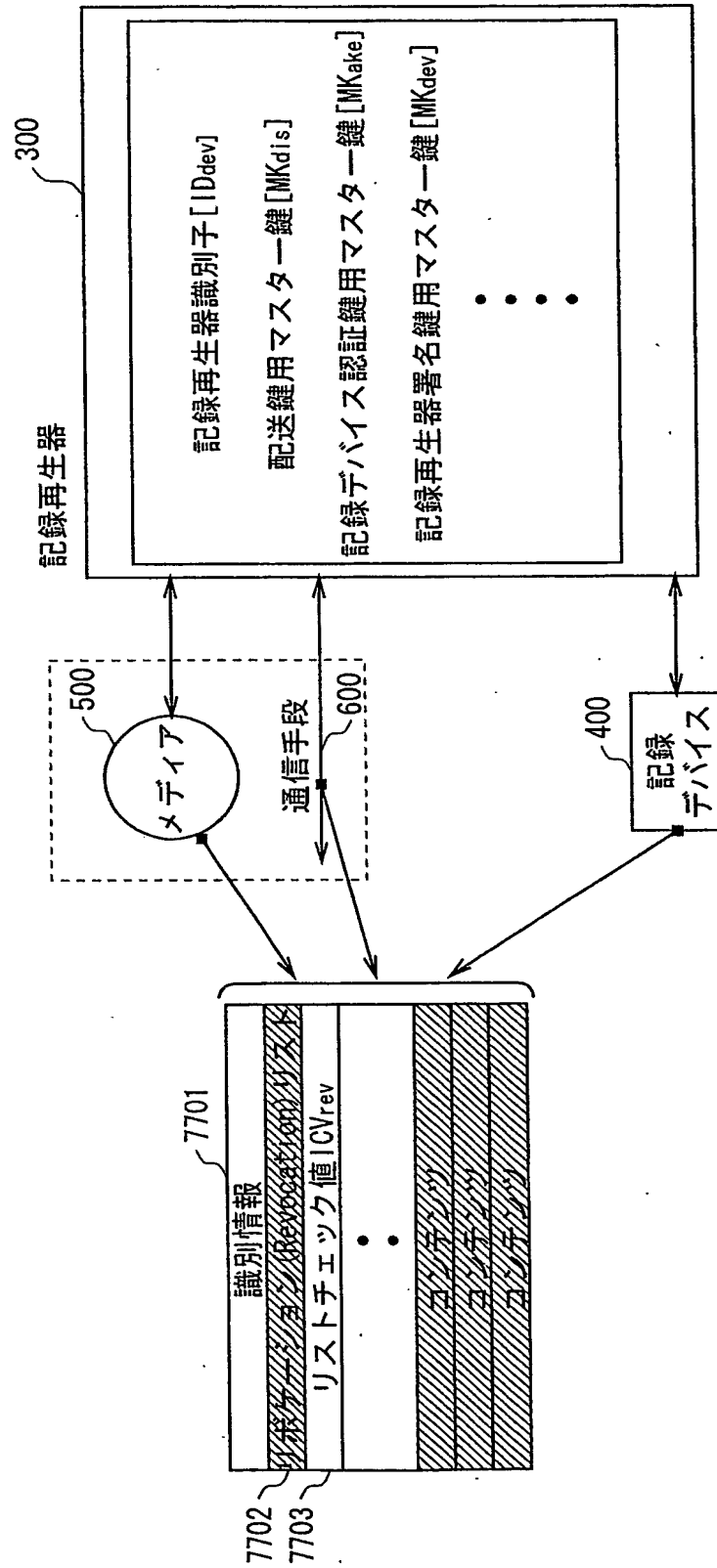


図 86

THIS PAGE BLANK (USPTO)

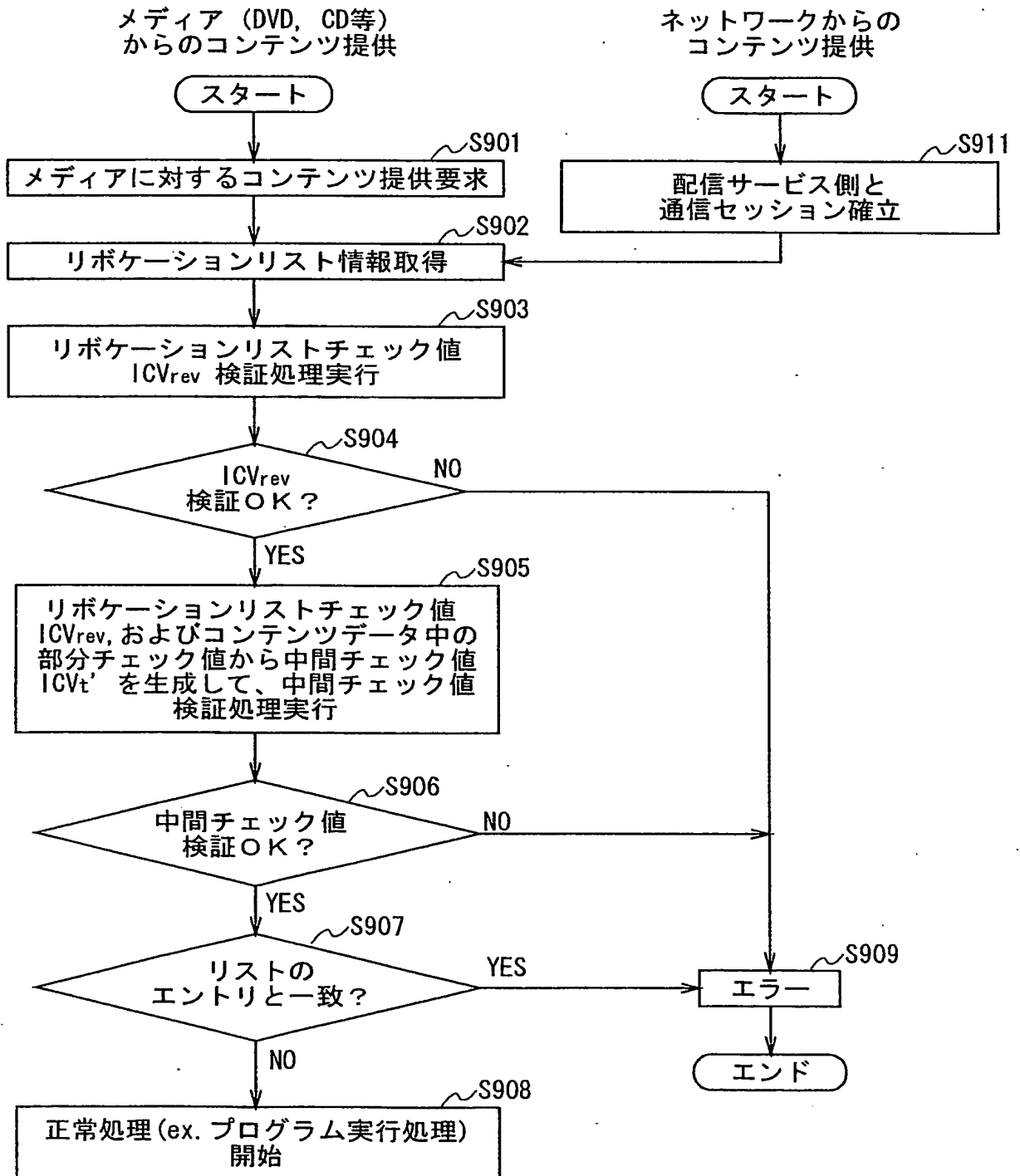


図 8 7

THIS PAGE BLANK (USPTO)

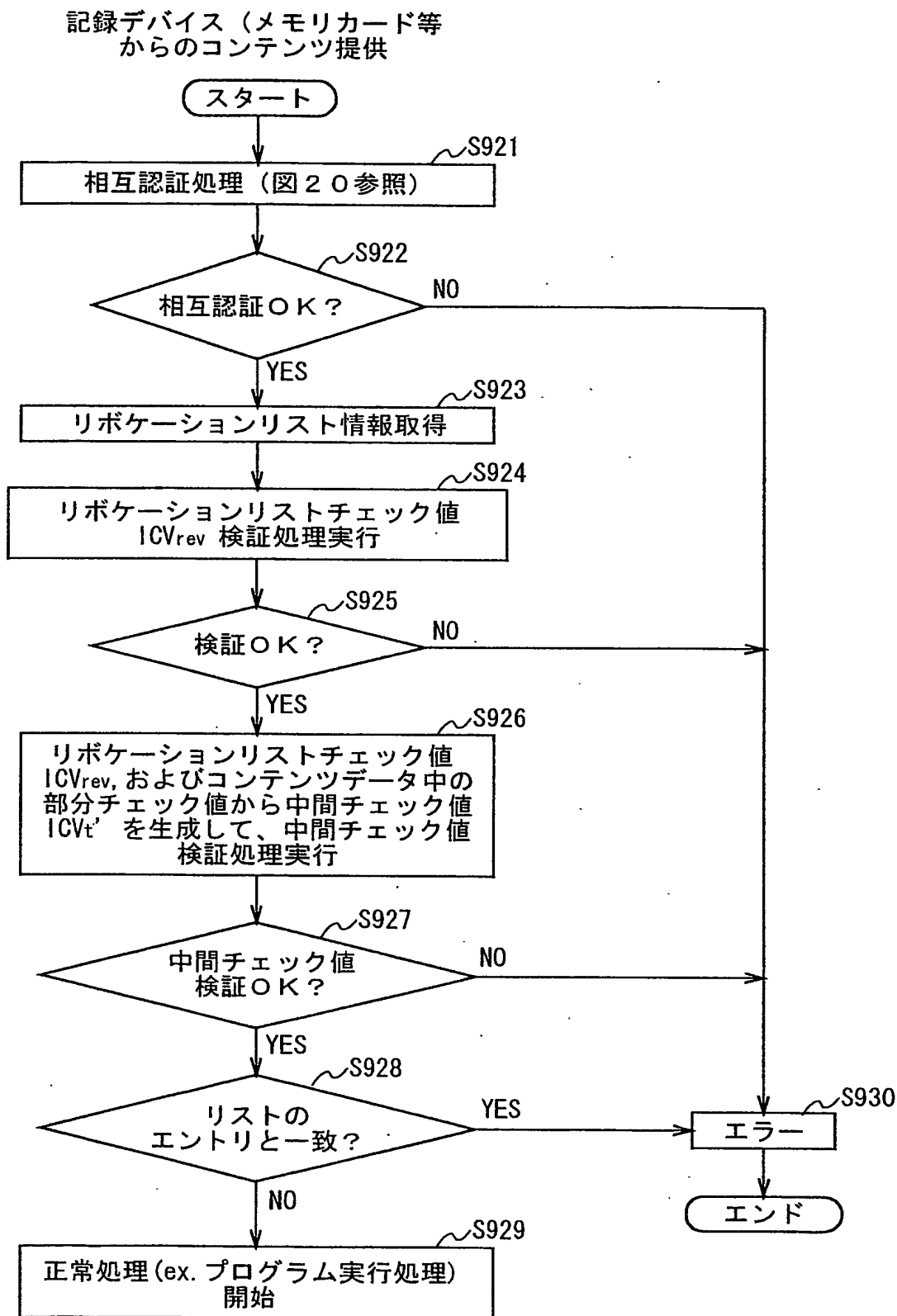


図88

THIS PAGE BLANK (uspto)

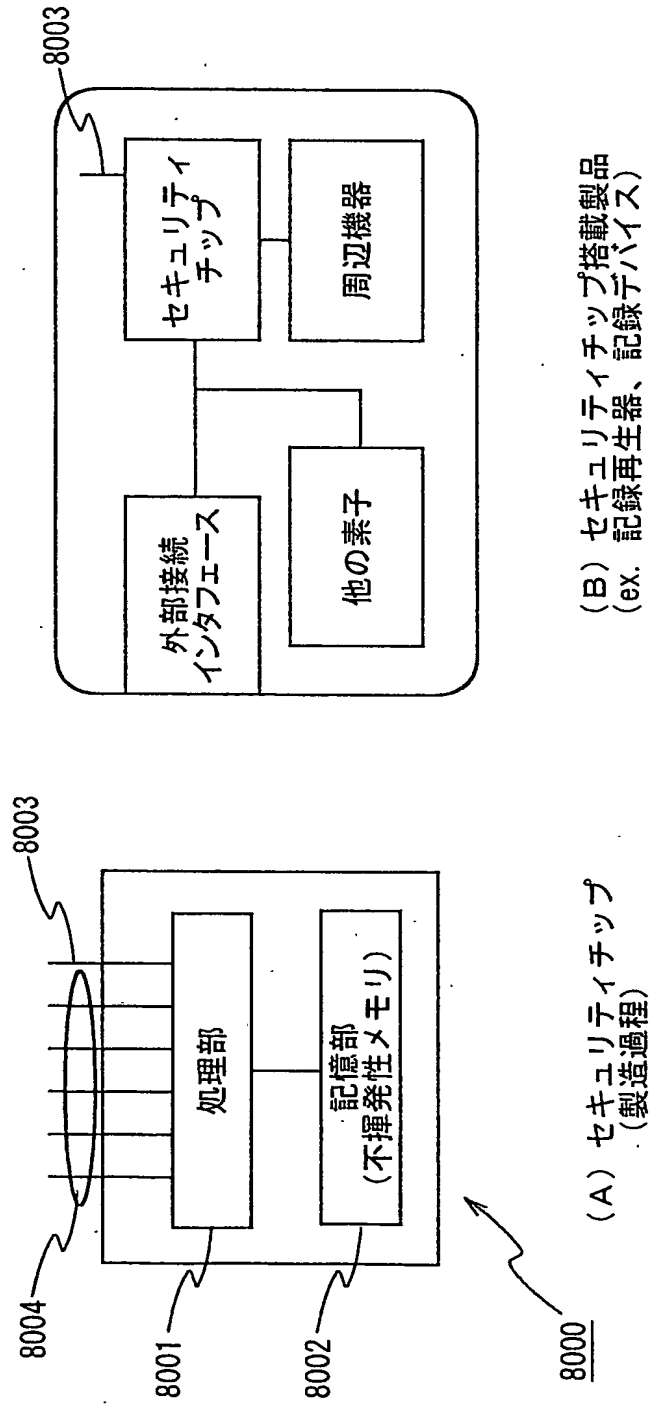


図 89

THIS PAGE BLANK (uspto)

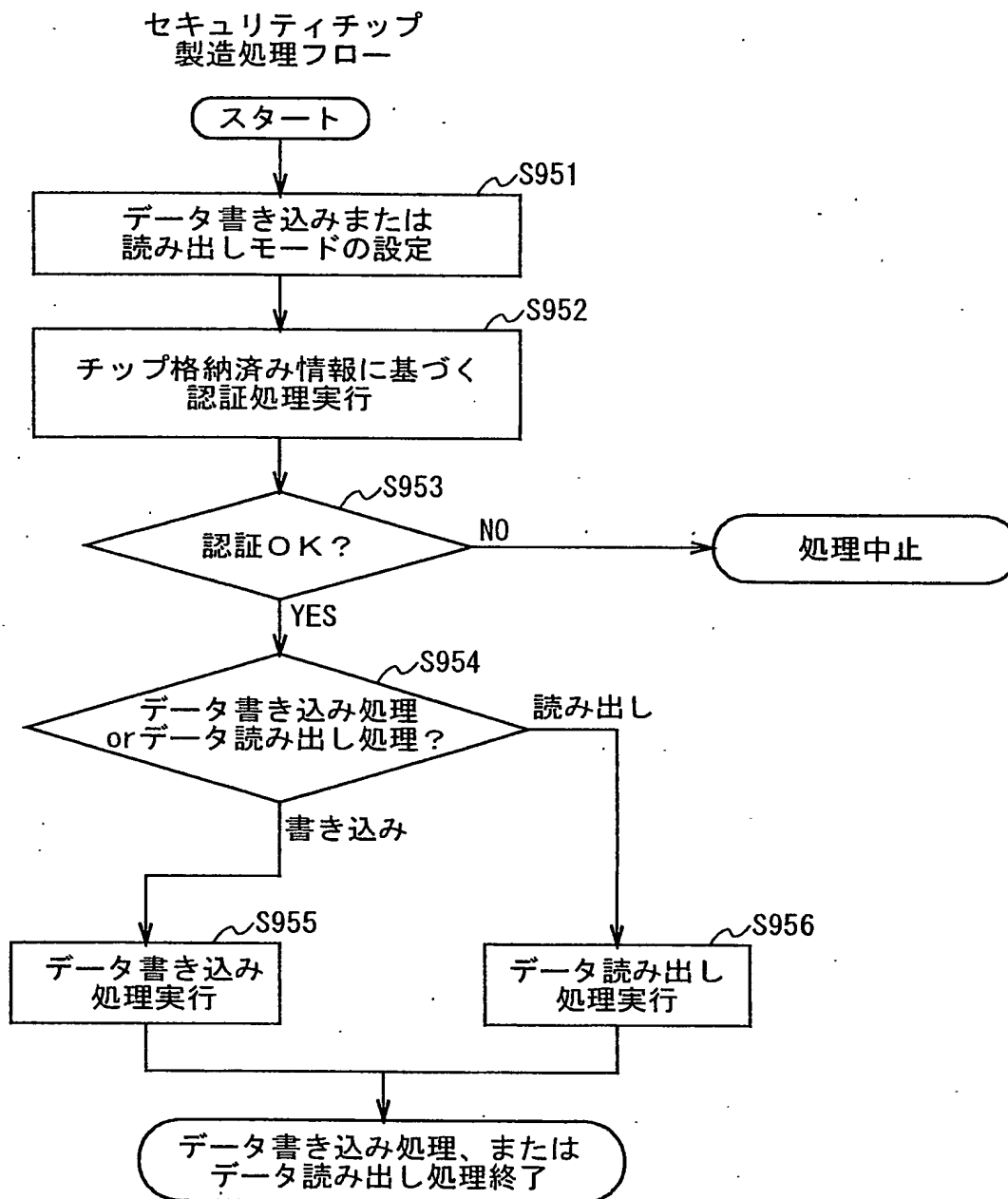


図 90

THIS PAGE BLANK (USPTO)

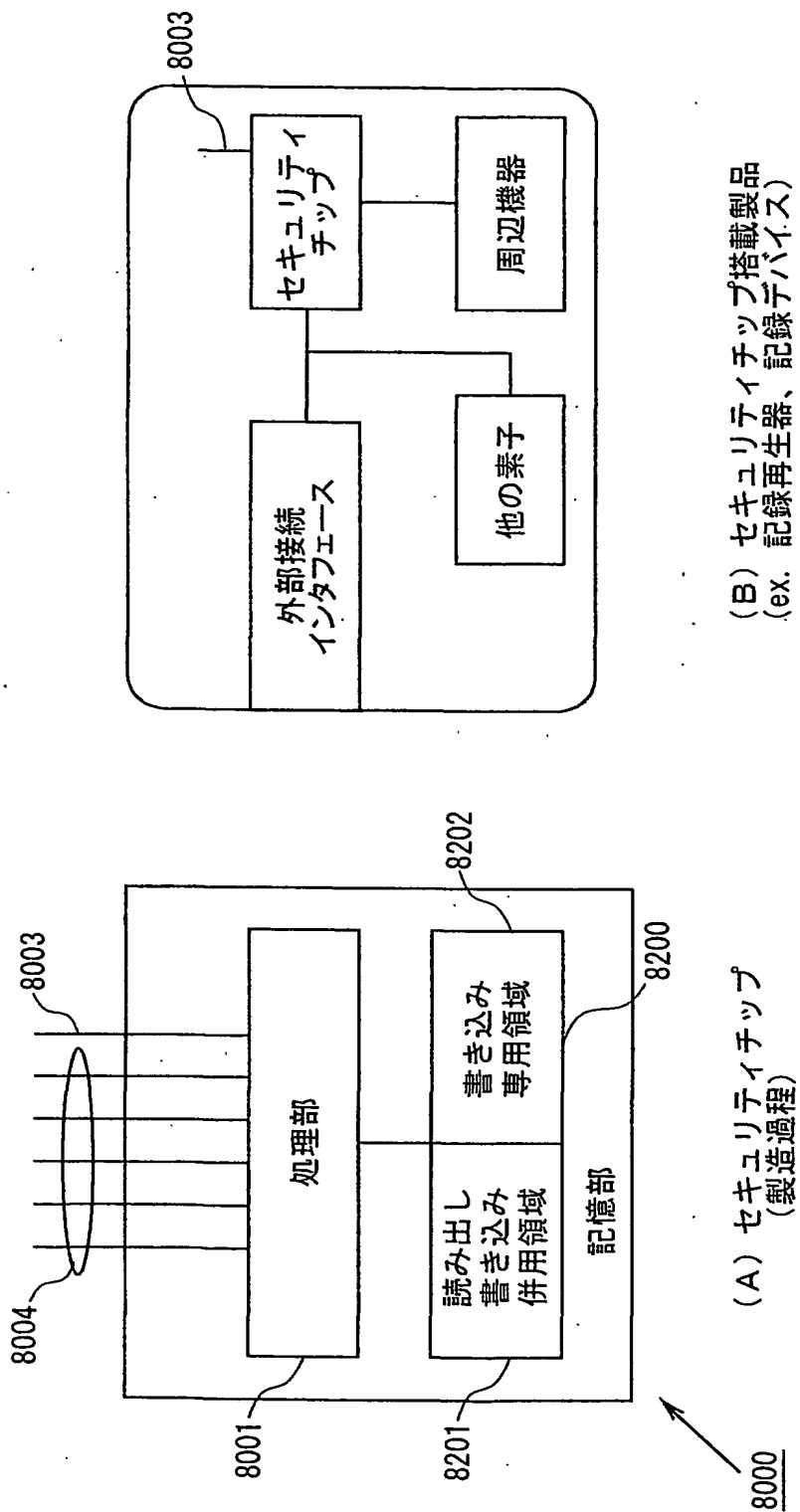


図 9 1

THIS PAGE BLANK (uspto)

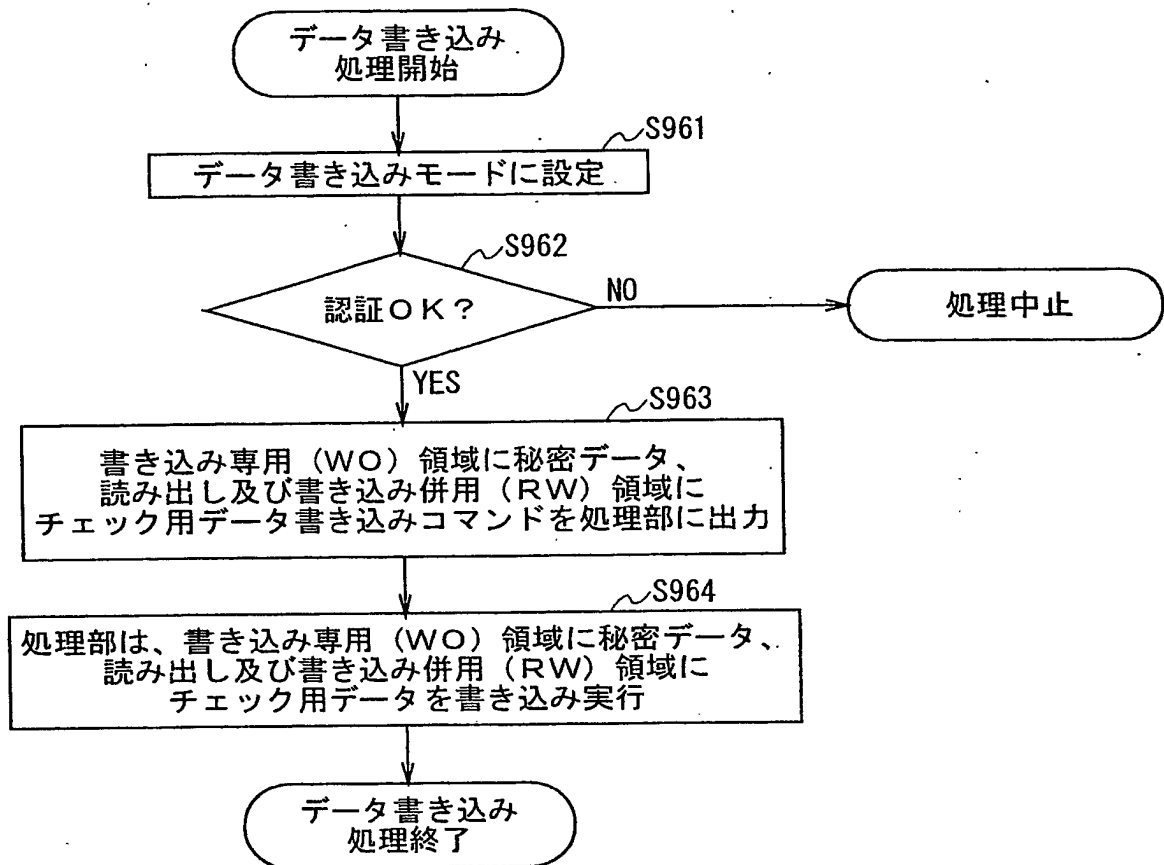


図 9 2

THIS PAGE BLANK (USPTO)

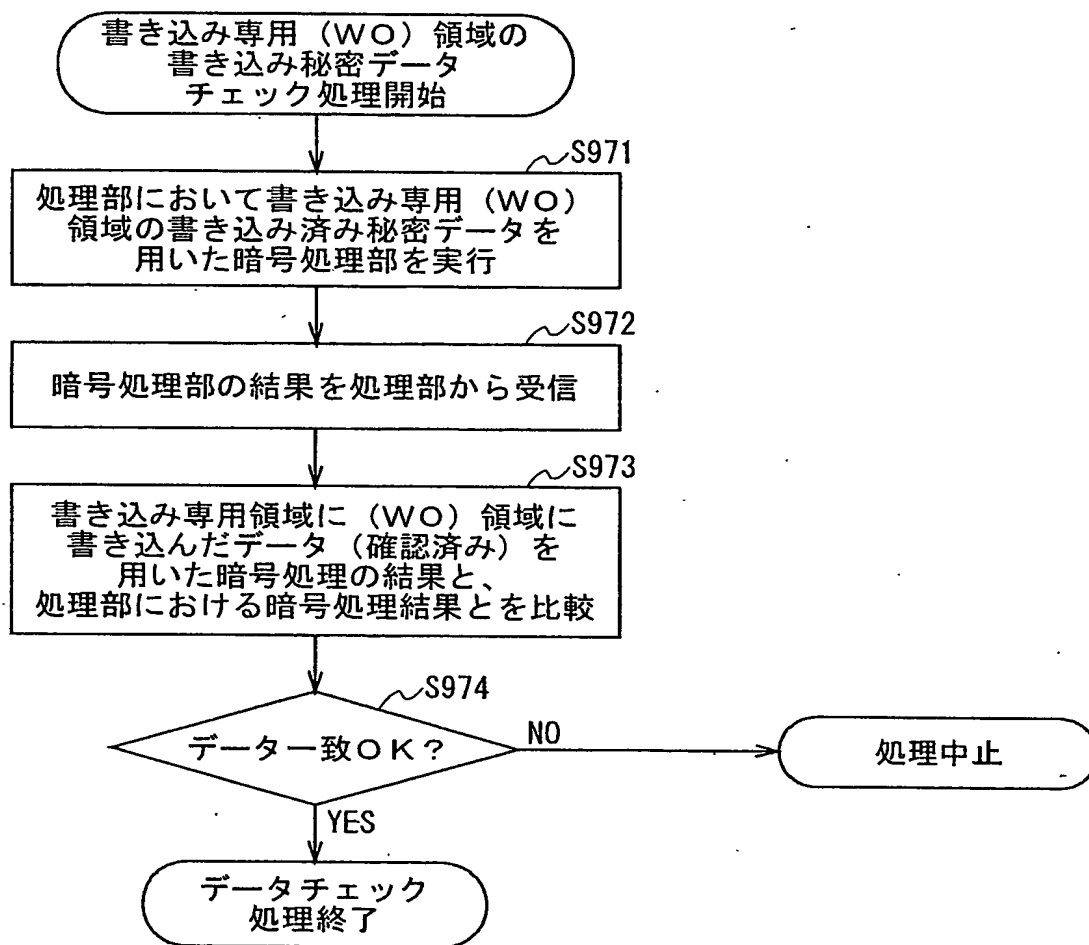


図 9 3

THIS PAGE BLANK (USPTO)

符 号 の 説 明

106……メインCPU、 107……RAM、 108……ROM、 109……AV処理部、 110……入力処理部、 111……PIO、 112……SIO、 300……記録再生器、 301……制御部、 302……暗号処理部、 303……記録デバイスコントローラ、 304……読み取り部、 305……通信部、 306……制御部、 307……内部メモリ、 308……暗号／復号化部、 400……記録デバイス、 401……暗号処理部、 402……外部メモリ、 403……制御部、 404……通信部、 405……内部メモリ、 406……暗号／復号化部、 407……外部メモリ制御部、 500……メディア、 600……通信手段、 2101, 2102, 2103……記録再生器、 2104, 2105, 2106……記録デバイス、 2901……コマンド番号管理部、 2902……コマンドレジスタ、 2903, 2904……認証フラグ、 3001……スピーカ、 3002……モニタ、 3090……メモリ、 3091……コンテンツ解析部、 3092……データ記憶部、 3093……プログラム記憶部、 3094……圧縮伸長処理部、 7701……コンテンツデータ、 7702……リボケーションリスト、 7703……リストチェック値、 8000……セキュリティチップ、 8001……処理部、 8002……記憶部、 8003……モード信号線、 8004……コマンド信号線、 8201……読み出し書き込み併用領域、 8202……書き込み専用領域

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00346

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G09C1/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G09C1/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 3-151738, A (Hitachi, Ltd.), 27 June, 1991 (27.06.91), Full text; all drawings (Family: none)	1-16, 20-33, 36-45, 86-100, 102-127, 128-135
Y	JP, 9-121340, A (Thomson Consumer Electronics Inc.), 06 May, 1997 (06.05.97), Par. Nos. [0005] to [0006]; Par. Nos. [0020] to [0072]; Figs. 1 to 12 & TR, 970038, A & EP, 752786, A & CN, 1146122, A & US, 5625693, A & BR, 9602980, A & ES, 214311, T & DE, 69606673, T	1-16, 20-33, 36-45
Y	JP, 8-248879, A (International Business Machines Corp.), 27 September, 1996 (27.09.96), Full text; all drawings & EP, 725511, A & US, 5673319, A	4-6, 22, 23, 39, 4 0, 106, 107, 119, 120, 131, 132
X	Shinichi IKENO et al., "Gendai Angou Riron" (the 3 rd printing), Zaidan Houjin, Denshi Jouhou Tsushin Gakkai,	17, 18, 34, 35

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not
considered to be of particular relevance
"E" earlier document but published on or after the international filing
date
"L" document which may throw doubts on priority claim(s) or which is
cited to establish the publication date of another citation or other
special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other
means
"P" document published prior to the international filing date but later
than the priority date claimed

"T" later document published after the international filing date or
priority date and not in conflict with the application but cited to
understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be
considered novel or cannot be considered to involve an inventive
step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be
considered to involve an inventive step when the document is
combined with one or more other such documents, such
combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
10 April, 2001 (10.04.01)

Date of mailing of the international search report
24 April, 2001 (24.04.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00346

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	20 May, 1989 (20.05.89) chapter 12, Digital Shomei no (2); Ninshoushi Shougou hou pp.223-225	
X	JP, 6-289782, A (Matsushita Electric Ind. Co., Ltd.), 07 April, 1993 (07.04.93), Par. Nos. [0009], [0017] to [0020], [0024]; Figs. 1-4	47,49,53,58, 60,67
Y	Par. Nos. [0014] to [0015]; Figs. 1-4 (Family: none)	48,50-52, 54-57,59,61-63
Y	Eiji OKAMOTO, "Angou Riron Numon" (the 1 st printing) Kyouritsu Shuppan K.K., 25 February, 1993 (25.02.93) chapter 6; Angoukagi Haisou Kanri Houshiki to Himitsu Jouhou Bunsan Houshiki (3); Kanri Bunsan gata Kagi Haisou Houshiki, "Mutsushin Type" deno "Taishou Kagi Seisei Houshiki" pp.118-119	48,51,52, 54-56,59,62, 64-66,83-100
Y	JP, 6-162289, A (Nippon Telegr. & Teleph. Corp. <NTT>), 10 June, 1994 (10.06.94), Par. Nos. [0008], [0010]; Figs. 1 to 7 & DE, 69322463, C & EP, 588339, A & US, 5396558, A & US, 5446796, A & US, 5502765, A & EP, 856821, A & EP, 856822, A	50,61,63
X	JP, 10-187826, A (NEC Corporation), 21 July, 1998 (21.07.98), Full text; all drawings	69,74,79,82
Y	Full text; all drawings (Family: none)	70-73,75-77, 80,81
Y	JP, 9-106429, A (Hitachi, Ltd.), 22 April, 1997 (22.04.97), Par. Nos. [0008], [0015] to [0017]; Fig. 1 (Family: none)	70-73,75-77, 80,81
Y	JP, 10-3257, A (Toshiba Corporation), 06 January, 1998 (06.01.98), Full text; all drawings & US, 5915024, A	128-135
X	JP, 10-126406, A (Toyo Communication Equipment Co., Ltd.), 15 May, 1998 (15.05.98), Full text; all drawings (Family: none)	137-151
X	JP, 10-283280, A (MVP K.K.), 23 October, 1998 (23.10.98), Full text; all drawings	153-155, 157-159, 161-165, 167-169,
Y	Full text; all drawings (Family: none)	171-174,176 156,160,166, 170,175,177
Y	JP, 10-164508, A (NEC Corporation), 19 June, 1998 (19.06.98), Par. Nos. [0020] to [0021], [0025]; Figs. 1 to 8	156,160,166, 170,175,177

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00346

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	& US, 6163647, A	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00346

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 46,68,82,101,136,152,178
because they relate to subject matter not required to be searched by this Authority, namely:
The inventions of claims 46, 68, 82, 101, 136, 152, 178 relate to a program source provided by means of a program providing medium, relating to mere presentation of information and to a subject matter required to be searched by this International Searching Authority according to PCT Article 17(2) (a) (i) and Rule 39.1(v).
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See "extra sheet"

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐

The additional search fees were accompanied by the applicant's protest.

☒

No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00346Continuation of Box No.II of continuation of first sheet (1)

The inventions of claims 1-16, 18-33 relate to a technique for verifying partial data and partial data sets through an electronic signature; the inventions of claims 17, 34 relate to a structure of a data processor having a verifying structure through an electronic signature; the inventions of claims 36-45 relate to a method for generating/imparting an electronic signature; the inventions of claims 47-67 relate to a data processor for performing encryption and electronic signature, a system structure, and a data processing method; the inventions of claims 69-78 relate to a data processor and a data processing method complying with electronic signature protocols; the inventions of claims 80, 81 relate to a method for creating content data having a function of excluding an unauthorized terminal; the inventions of claims 83-100 relate to a structure of a data processor; the inventions of claims 102-127 relate to a structure of a data processor having a structure for verifying an electronic signature of content data and a data processing method; the inventions of claims 128-135 relate to a method for creating/imparting an electronic signature for processing content data; the inventions of claims 137-139 relate to a data processor for performing encryption and electronic signature; the inventions of claims 140-151 relate to a method for creating content data which is encrypted and to which an electronic signature is imparted; and the inventions of claims 153-178 relate to a structure of a data processor for compressing/decompressing content data and a data processing method. The gists of the groups of inventions of claims 1-178 are independent of one another, and therefore these groups of inventions are not so linked as to form a single general inventive concept.

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G09C1/00, H04L9/32

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G09C1/00, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 3-151738, A (株式会社日立製作所) 27. 6月. 1991 (27. 06. 91) 全文, 全図 (ファミリーなし)	1-16, 20-33, 3 6-45, 86-100, 102-127, 128- 135
Y	J P, 9-121340, A (トムソン コンシューマ エレク トロニクス インコーポレイテッド) 6. 5月. 1997 (06. 05. 97) 第【0005】-【0006】段落,	1-16, 20-33, 3 6-45

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

10. 04. 01

国際調査報告の発送日

24.04.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	第【0020】－【0072】段落, 図1－12 & TR, 970038, A & EP, 752786, A & CN, 1146122, A & US, 5625693, A & BR, 9602980, A & ES, 214311, T & DE, 69606673, T	
Y	JP, 8-248879, A (インターナショナル・ビジネス・ マシーンズ・コーポレーション) 27. 9月. 1996 (27. 09. 96) 全文, 全図 & EP, 725511, A & US, 5673319, A	4-6, 22, 23, 3 9, 40, 106, 10 7, 119, 120, 13 1, 132
X	池野信一, 小山謙二 著: “現代暗号理論” (3版) 財団法人 電子情報通信学会 発行, 20. 5月. 1989 (20. 05. 89) 第12章デジタル署名の(2) 認証子照合法 p. 223-225	17, 18, 34, 35
X	JP, 6-289782, A (松下電器産業株式会社) 7. 4月. 1993 (07. 04. 93)	
Y	第【0009】段落, 第【0017】－【0020】段落, 第【0024】段落, 図1-4 第【0014】－【0015】段落, 図1-4 (ファミリーなし)	47, 49, 53, 58, 60, 67 48, 50-52, 54- 57, 59, 61-63
Y	岡本栄司 著: “暗号理論入門” (初版1刷) 共立出版株式会社 発行, 25. 2月. 1993 (25. 02. 93) 第6章 暗号鍵配送管理方式と秘密情報分散方式の(3) 管理分散 型鍵配送方式、「無通信タイプ」での「対称鍵生成方式」を参照 p. 118-119	48, 51, 52, 54- 56, 59, 62, 64- 66, 83-100
Y	JP, 6-162289, A (日本電信電話株式会社) 10. 6月. 1994 (10. 06. 94) 第【0008】段落, 第【0010】段落, 図1-7 & DE, 69322463, C & EP, 588339, A & US, 5396558, A & US, 5446796, A & US, 5502765, A & EP, 856821, A & EP, 856822, A	50, 61, 63

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	J P, 10-187826, A (日本電気株式会社) 21. 7月. 1998 (21. 07. 98) 全文, 全図 全文, 全図 (ファミリーなし)	69, 74, 79, 82 70-73, 75-77, 80, 81
Y	J P, 9-106429, A (株式会社日立製作所) 22. 4月. 1997 (22. 04. 97) 第【0008】段落, 第【0015】 - 【0017】段落, 図1 (ファミリーなし)	70-73, 75-77, 80, 81
Y	J P, 10-3257, A (株式会社東芝) 6. 1月. 1998 (06. 01. 98) 全文, 全図 & US, 5915024, A	128-135
X	J P, 10-126406, A (東洋通信機株式会社) 15. 5月. 1998 (15. 05. 98) 全文, 全図 (ファミリーなし)	137-151
X	J P, 10-283280, A (エムブイピー株式会社) 23. 10月. 1998 (23. 10. 98) 全文, 全図	153-155, 157- 159, 161-165, 167-169, 171- 174, 176
Y	全文, 全図 (ファミリーなし)	156, 160, 166, 170, 175, 177
Y	J P, 10-164508, A (日本電気株式会社) 19. 6月. 1998 (19. 06. 98) 第【0020】 - 【0021】段落, 第【0025】段落, 図1-8 & US, 6163647, A	156, 160, 166, 170, 175, 177

第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☒ 請求の範囲 46, 68, 82, 101, 136, 152, 178 は、この国際調査機関が調査することを要しない対象に係るものである。つまり、請求の範囲 46, 68, 82, 101, 136, 152, 178 は、プログラム提供媒体にて提供されるプログラムソースであり、情報の単なる提示に該当し、PCT (2)(a) (i) 及び PCT 規則 39.1 (v) の規定により、この国際調査機関が調査することを要しないものに係るものである。
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であって PCT 規則 6.4(a) の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

「特別ページ」を参照

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

請求の範囲1-16, 18-33は、部分データ及び部分データ群それぞれに対する電子署名での検証技術について記載した発明であるのに対し、請求の範囲17, 34は電子署名による検証構成を有するデータ処理装置の構成が、請求の範囲36-45は電子署名の生成及び付与方法が、請求の範囲47-67は暗号と電子署名を行うデータ処理装置やシステムの構成乃至データ処理方法が、請求の範囲69-78は電子署名プロトコルによるデータ処理装置乃至データ処理方法が、請求の範囲80-81は不正端末の排除機能を備えたコンテンツデータの生成方法が、請求の範囲83-100はデータ処理装置の構成が、請求の範囲102-127はコンテンツデータに対する電子署名の検証構成を有するデータ処理装置の構成乃至データ処理方法が、請求の範囲128-135はコンテンツデータ処理のための電子署名の生成、付与方法が、請求の範囲137-139は暗号処理と電子署名とを行うデータ処理装置が、請求の範囲140-151は暗号処理と電子署名付与を施されたコンテンツデータの生成方法が、請求の範囲153-178はコンテンツデータの圧縮、伸長処理を行うデータ処理装置の構成乃至データ処理方法が記載されており、その要旨がそれぞれ異なった独立した発明として成立することから、請求の範囲1-178は単一の発明について記載したものではない。

THIS PAGE BLANK (USPTO)